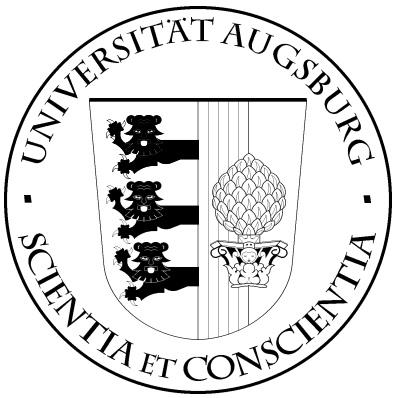
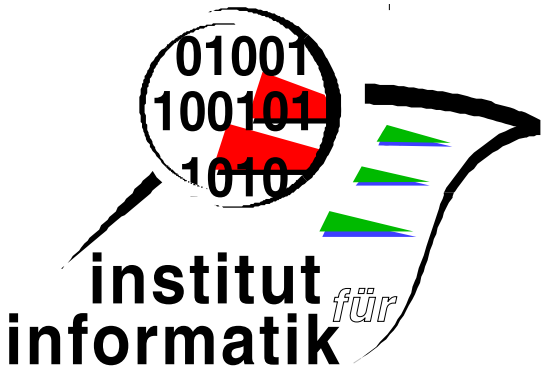
Universität Augsburg



Kleene under a Modal Demonic Star

Jules Desharnais **Bernhard Möller** **Fairouz Tchier**

Report 2004-11 Mai 2004



Institut für Informatik
D-86135 Augsburg

Kleene Under a Modal Demonic Star

Jules Desharnais [a], Bernhard Möller [b], Fairouz Tchier [c]

[a] *Département d'informatique, Université Laval, Québec QC G1K 7P4 Canada*

[b] *Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany*

[c] *Mathematics Department, King Saud University, P.O.Box 22452, Riyadh 11495, Saudi Arabia*

Abstract

In relational semantics, the input-output semantics of a program is a relation on its set of states. We generalize this in considering elements of Kleene algebras as semantical values. In a nondeterministic context, the *demonic* semantics is calculated by considering the worst behavior of the program. In this paper, we concentrate on while loops. *Calculating* the semantics of a loop is difficult, but *showing the correctness* of any candidate abstraction is much easier. For deterministic programs, Mills has described a checking method known as the *while statement verification rule*. A corresponding programming theorem for nondeterministic iterative constructs is proposed, proved and applied to an example. This theorem can be considered as a generalization of the while statement verification rule to nondeterministic loops. The paper generalizes earlier relation-algebraic work to the setting of *modal Kleene algebra*, an extension of Kozen's Kleene algebra with tests that allows the internalization of weakest liberal precondition and strongest liberal postcondition operators.

Key words: while loop, demonic semantics, relational abstraction, verification, Kleene algebra, rule, generalization.

1 Introduction

We use elements of Kleene algebras as abstractions of the input-output semantics of nondeterministic programs. In the concrete Kleene algebra of homogeneous binary relations, the operators $\cup$ and ; have been used for many

Email addresses: Jules.Desharnais@ift.ulaval.ca (Jules Desharnais), Bernhard.Moeller@informatik.uni-augsburg.de (Bernhard Möller), ftchier@hotmail.com (Fairouz Tchier).

years to define the so-called *angelic semantics*, which assumes that a program goes right when there is a possibility to go right. The *demonic choice* $\sqcup$ and *demonic composition* $\diamond$ do the opposite: if there is a possibility to go wrong, a program whose semantics is given by these operators goes wrong. The demonic semantics of a while loop is given as a fixed point of an isotone function involving the demonic operators.

While there is no systematic way to calculate the relational abstraction of a while loop directly from the definition, it is possible to check the correctness of any candidate abstraction. For deterministic programs, Mills [22,23] has described a checking method known as the *while statement verification rule*. We generalize this rule to nondeterministic loops.

We note here that half of the generalized theorem has been shown by Sekerinski [31], who uses an approach based on predicative programming [18]. A related theorem has been given by Norvell [28] in the framework of predicative programming with time bounds. Norvell's theorem shows how to refine the specification R of a while loop under the condition that R is *strongly bounded*, which guarantees termination after a finite amount of time. Further refinement theorems for loops can be found in [1], presented in the framework of predicate transformers.

The main novelties in the present paper are the following. First, we fully generalize Mills's approach to the nondeterministic case. This was already achieved by Desharnais and Tchier [33,34] using binary homogeneous relations. Second, at the same time we abstract from relational semantics to the more general setting of modal Kleene algebras, an extension of Kozen's Kleene algebra with tests [20] that allows the internalization of the abstract counterparts of the weakest liberal precondition and strongest liberal postcondition operators. A first treatment of this topic in the more restricted class of Standard Kleene Algebras [8] appeared in [14]; in the present paper we show that we can do without the assumption that the underlying lattice forms a complete Boolean algebra and that sequential composition is universally disjunctive. In doing so, we present some derived operations and laws that will also be useful for further applications of modal Kleene algebra. It is remarkable that the proofs in the generalized setting are considerably simpler and more perspicuous than the corresponding ones in terms of relations or predicate transformers.

The rest of this paper is organized as follows. In Section 2 we first introduce test semirings; they admit a direct abstract angelic semantics of loop-free programs. Next, we axiomatize a domain and a codomain operation [11] that assign to an abstract program a representation of its initial and final states, respectively. Based on that, forward and backward diamond and box operators can be defined, leading to modal semirings. The forward operators correspond to the strongest liberal postcondition and weakest liberal precondition oper-

ators. In Section 3 we then give the abstract demonic semantics of loop-free programs and show a number of basic properties such as associativity of demonic composition. In Section 4, we introduce finite and infinite iteration, leading to modal Kleene [13] and omega [7,26] algebras and show a number of auxiliary properties. Following that, we present in Section 5 a generalization of the *while statement verification rule* of Mills. This is followed by an example of application in Section 6. The paper terminates with a conclusion in Section 7.

2 Domain Semirings and Modalities

2.1 Test Semirings

Definition 2.1 *(a) A* semiring *is a structure* $(K, +, \cdot, 0, 1)$ *such that* $(K, +, 0)$ *is a commutative monoid,* $(K, \cdot, 1)$ *is a monoid, multiplication distributes over addition from the left and right and zero is a left and right annihilator, i.e.,* $a \cdot 0 = 0 = 0 \cdot a$ *for all* $a \in K$.

(b) The semiring is idempotent *if it satisfies* $a + a = a$ *for all* $a \in K$. *Then* K *has a* natural ordering $\leq$ *defined for all* $a, b \in K$ *by* $a \leq b$ *iff* $a + b = b$. *It induces a semilattice with* $+$ *as join and* 0 *as the least element; addition and multiplication are isotone with respect to the natural ordering.*

In many contexts these operations can be interpreted as follows:

$+$ $\leftrightarrow$ choice,
$\cdot$ $\leftrightarrow$ sequential composition,
0 $\leftrightarrow$ abortion,
1 $\leftrightarrow$ identity,
$\leq$ $\leftrightarrow$ increase in information or in choices.

Example 2.2 *(a) The basis of Kleene's original work on regular algebra is the semiring* $\mathrm{LAN} \triangleq (\mathcal{P}(A^*), \cup, \bullet, \emptyset, \varepsilon)$, *of formal languages over some alphabet* A, *where* A^* *is the set of all finite words over* A, $\bullet$ *denotes concatenation and* ε *the empty word (as usual, we identify a singleton language with its only element).*

(b) Another important KA is $\mathrm{REL} \triangleq (\mathcal{P}(M \times M), \subseteq, M \times M, ;, \emptyset, I)$, *the algebra of homogeneous binary relations over some set* M *under relational composition* ; . *More generally than the concrete relation algebra* REL, *every abstract relation algebra (see e.g. [6,30,32]) is a KA.*

(c) A less abstract semiring than REL *is the semiring* PAT *of path sets in a directed graph under union as addition and the extension of path concatenation to path sets (also known as fusion product) as multiplication (see e.g. [25] for details). Whereas* REL *only gives information about ex-*

istence of a path between a pair of nodes, PAT *gives the possibility to talk about different paths between that same pair.*

□

Programs and state transition systems can be described in a bipartite world in which propositions describe sets of states and actions or events model transitions between states. Propositions live in a Boolean algebra and actions in an idempotent semiring with the operations interpreted as above. In fact, to model regular programs, an additional operation of iteration or reflexive transitive closure is required; the corresponding extension of semirings to Kleene algebras is described in Section 4. The idea to combine propositions and actions into one common framework was first presented in Kozen's Kleene algebra with tests [20], where "test" is a synonym for "proposition". Let us now axiomatize the corresponding notions.

Definition 2.3 *(a) A* Boolean algebra *is a complemented distributive lattice. By overloading, we usually write* $+$ *and* $\cdot$ *also for the Boolean join and meet operation and use* 0 *and* 1 *for the least and greatest elements of the lattice. The symbol* $\neg$ *denotes the operation of complementation.*

(b) A test semiring *is a two-sorted structure* $(K, \mathsf{test}(K))$*, where* K *is an idempotent semiring and* $\mathsf{test}(K) \subseteq K$ *is a Boolean algebra embedded into* K *such that the operations of* $\mathsf{test}(K)$ *coincide with the restrictions of the operations of* K *to* $\mathsf{test}(K)$*. In particular,* $p \leq 1$ *for all* $p \in \mathsf{test}(K)$*. But in general,* $\mathsf{test}(K)$ *is only a subalgebra of the subalgebra of all elements below* 1 *in* K*.*

We will use the letters $a, b, c, \ldots$ for semiring elements and $p, q, r, \ldots$ for Boolean elements. We will freely use the concepts and laws associated with Boolean algebra, including relative complement $p - q = p \cdot \neg q$ and implication $p \rightarrow q = \neg p + q$.

Example 2.4 *(a) In* LAN*, the only possible tests are* $\emptyset$ *and* $\{\varepsilon\}$*, i.e.,* 0 *and* 1*. Such a semiring is said to have a* discrete *test algebra, which usually is not very interesting.*

(b) In REL *usually the set of all partial identity relations is chosen as the test algebra to make it a test semiring.*

(c) In PAT *one chooses the tests to be all sets that consist of paths with at most one node each. Except for the empty path, such sets are isomorphic to sets of points.* □

In a test semiring one can give (angelic) abstract semantics of repetition-free

programs as follows:

$$\begin{aligned}
\mathsf{abort} &\triangleq 0 \\
\mathsf{skip} &\triangleq 1 \\
a \,[]\, b &\triangleq a + b \\
a \,;\, b &\triangleq a \cdot b \\
\mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b &\triangleq p \cdot a + \neg p \cdot b \\
\mathsf{assert}\ p &\triangleq \mathsf{if}\ p\ \mathsf{then\ skip\ else\ abort} \;=\; p
\end{aligned}$$

The definition of $\mathsf{assert}\ p$ via $\mathsf{if\ then\ else}$ is the usual one from assertion macro packages in programming languages like *C* or *Java*; algebraically it simplifies to p alone.

2.2 Domain

In many formalisms, propositions and actions cooperate via modal operators that view actions as mappings on propositions in order to describe state-change and via test operators that embed propositions into actions in order to describe measurements on states and to model the usual program constructs.

To motivate this modal view, let a semiring element a describe an action or abstract program and a test p a proposition or assertion, also called a *test*. Then $p \cdot a$ describes a restricted program that acts like a when the initial state satisfies p and aborts otherwise. Symmetrically, $a \cdot p$ describes a restriction of a in its possible final states. We now introduce an abstract domain operator $\ulcorner$ [24] that assigns to a the test that describes precisely its enabling states.

Definition 2.5 *A* semiring with domain *[11] (a $\ulcorner$-semiring) is a structure $(K, \ulcorner)$, where K is an idempotent semiring and the* domain operation $\ulcorner\colon K \to \mathsf{test}(K)$ *satisfies for all $a, b \in K$ and $p \in \mathsf{test}(K)$*

$$a \leq \ulcorner a \cdot a, \tag{d1}$$
$$\ulcorner(p \cdot a) \leq p. \tag{d2}$$

Let us explain these axioms. First, since $\ulcorner a \leq 1$ by $\ulcorner a \in \mathsf{test}(K)$, isotonicity of multiplication shows that (d1) can be strengthened to an equality expressing that restriction to the full domain is no restriction at all. The second axiom means that after restriction the remaining domain must satisfy the restricting test.

To further explain (d1) and (d2) we note that their conjunction is equivalent

to each of

$$\ulcorner a \leq p \Leftrightarrow a \leq p \cdot a, \tag{llp}$$
$$\ulcorner a \leq p \Leftrightarrow \neg p \cdot a \leq 0, \tag{gla}$$

which constitute elimination laws for $\ulcorner$. (llp) says that $\ulcorner a$ is the least left preserver of a. (gla) says that $\neg\ulcorner a$ is the greatest left annihilator of a. Both properties obviously characterize domain in set-theoretic relations.

Because of (llp), domain is uniquely characterised by the two domain axioms. Moreover, if $\mathsf{test}(K)$ is complete then a domain operation always exists. If $\mathsf{test}(K)$ is not complete, this need not be the case. Another important consequence of the axioms is that $\ulcorner$ preserves arbitrary existing suprema [27].

Example 2.6 *(a) In* LAN*, the domain of a language L is $\emptyset$ if $L = \emptyset$ and $\{\varepsilon\}$ otherwise; i.e., domain decides merely about being* 0 *or not. The same applies to all test semirings with discrete test algebra.*

(b) A prominent example of a domain semiring is REL*. There, the domain operation is given by $\ulcorner R = R\,;R^{\smile} \cap I$, where I is the identity relation, $R^{\smile}$ is the converse of R and ; is relational composition.*

(c) In PAT*, the domain of a path set consists of all starting points of paths in the set, plus the empty path if it is in the path set.* □

Many natural properties follow from the axioms. Domain is uniquely defined. It is strict ($\ulcorner a = 0 \Leftrightarrow a = 0$), additive ($\ulcorner(a + b) = \ulcorner a + \ulcorner b$), isotone ($a \leq b \Rightarrow \ulcorner a \leq \ulcorner b$), stable on tests ($\ulcorner p = p$) and satisfies the import/export law ($\ulcorner(p \cdot a) = p \cdot \ulcorner a$). See [11] for further information. Moreover, we have a useful decomposition property.

Lemma 2.7 *For $p \in \mathsf{test}(K)$,*

$$a \leq p \cdot b \;\Leftrightarrow\; \ulcorner a \leq p \wedge a \leq b.$$

PROOF. ($\Rightarrow$) First, by isotonicity of domain and (d2), $\ulcorner a \leq \ulcorner(p \cdot b) \leq p$. Second, by $p \leq 1$ and isotonicity of $\cdot$ we have $a \leq b$ as well.
($\Leftarrow$) By (d1) and isotonicity of $\cdot$, $a \leq \ulcorner a \cdot a \leq p \cdot b$. □

2.3 Modal Semirings

Definition 2.8 *A domain semiring is called* modal *if additionally it satisfies*

$$\ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b). \tag{d3}$$

This axiom serves to make composition of multimodal operators below well-behaved. In a modal semiring, domain is *local* in the following sense:

$$\ulcorner(a \cdot b) = \ulcorner(a \cdot \ulcorner b). \tag{loc}$$

Without (d3), only the inequality $\ulcorner(a \cdot b) \leq \ulcorner(a \cdot \ulcorner b)$ holds. The additional axiom (d3) guarantees that the domain of $a \cdot b$ is independent of the inner structure of b or its codomain; information about the domain of b in interaction with a suffices.

Definition 2.9 *A codomain operation $\urcorner$ can easily be defined as a domain operation in the opposite semiring, where, as usual in algebra, opposition just swaps the order of multiplication. We call a semiring K with local domain and codomain simply a* modal semiring.

Combined with restriction, the domain operation yields an abstract preimage operation. This provides the semantic basis for defining modalities.

Definition 2.10 *Let K be a modal semiring. For all $a \in K$ and $p \in \mathsf{test}(K)$ we define*

$$|a\rangle p = \ulcorner(a \cdot p), \qquad\qquad \langle a|p = (p \cdot a)\urcorner.$$

Let us explain why this definition is adequate. For program a, the term $a \cdot p$ restricts a to that part for which all final states satisfy p. Then $\ulcorner(a \cdot p)$ selects all starting states of this remaining part; they indeed form the inverse image of p under a. Symmetric arguments apply to the backward diamond.

Duality with respect to opposition transforms forward diamonds into backward diamonds and vice versa. It follows that they satisfy an *exchange law*, a weak analogue of the relational Schröder law. For all $a \in K$ and $p, q \in \mathsf{test}(K)$,

$$|a\rangle p \leq \neg q \Leftrightarrow \langle a|q \leq \neg p. \tag{1}$$

De Morgan duality transforms diamonds into boxes and vice versa.

Definition 2.11

$$|a]p \triangleq \neg|a\rangle\neg p, \qquad\qquad [a|p \triangleq \neg\langle a|\neg p.$$

Example 2.12 *In the modal semiring* REL*, the forward box operator coincides with the* monotype factor *as defined by Backhouse and van der Woude in [3].* □

In the sequel, when the direction of diamonds and boxes does not matter, we will use the notation $\langle a\rangle$ and $[a]$.

From (1) it follows that diamonds (boxes) are lower (upper) adjoints of Galois connections:

$$|a\rangle p \leq q \Leftrightarrow p \leq [a|q, \qquad\qquad \langle a|p \leq q \Leftrightarrow p \leq |a]q, \tag{2}$$

for all $a \in K$ and $p, q \in \mathsf{test}(K)$. Hence diamonds (boxes) commute with all existing suprema (infima) of the test algebra. In particular,

$$\langle a\rangle(p+q) = \langle a\rangle p + \langle a\rangle q, \qquad\qquad [a](p \cdot q) = [a]p \cdot [a]q. \tag{3}$$

Further useful properties are immediate from the Galois connection. They include cancellation laws and isotonicity and antitonicity properties for modalities (see [13] for details). Of particular interest are the following demodalization laws that follow from the domain elimination law (gla) and its dual for codomain.

$$|a\rangle p \leq q \Leftrightarrow \neg q \cdot a \cdot p \leq 0, \qquad\qquad \langle a|p \leq q \Leftrightarrow p \cdot a \cdot \neg q \leq 0. \tag{4}$$

For a test p we have

$$\langle p\rangle q = p \cdot q, \qquad [p]q = p \rightarrow q. \tag{5}$$

Hence, $\langle 1\rangle = [1]$ is the identity function on tests. Moreover, $\langle 0\rangle p = 0$ and $[0]p = 1$.

Many modal properties can be expressed and calculated more succinctly in a point-free style at the level of the operator semirings induced by the modal operators. To this end, we lift join and meet pointwise to the operator level, setting for test transformers $f, g : \mathsf{test}(K) \rightarrow \mathsf{test}(K)$,

$$(f+g)(p) \stackrel{\triangle}{=} f(p) + g(p), \qquad (f \sqcap g)(p) = f(p) \cdot g(p).$$

Then we have the following properties:

$$\langle a+b\rangle = \langle a\rangle + \langle b\rangle, \qquad [a+b] = [a] \sqcap [b]. \tag{6}$$

The definition

$$f \leq g \stackrel{\triangle}{\Leftrightarrow} f + g = g$$

lifts the natural order pointwise to test transformers, i.e., $f \leq g \Leftrightarrow \forall(p :: f(p) \leq g(p))$. Now, from (6) it follows that $\langle \_\rangle$ is isotone and $[\_]$ is antitone.

Further, we denote composition of modal operators by mere juxtaposition.

Then the modal axiom (d3) implies

$$\left.\begin{aligned} |a \cdot b\rangle &= |a\rangle|b\rangle, \quad \langle a \cdot b| = \langle b|\langle a|, \\ |a \cdot b] &= |a]|b], \quad [a \cdot b| = [b|[a|. \end{aligned}\right\} \tag{7}$$

Thus multiplication acts covariantly on forward modalities and contravariantly on backward ones.

2.4 Test Implication

The following operator, a combination of domain and the forward box operator, will be instrumental in propagating assertions through compositions. It mainly serves to smoothen the notation; this is best exemplified with the proof of Theorem 3.8 below, which would be quite messy in the original notation of modal operators.

Definition 2.13 *The binary operator* $\rightarrow$*, called* test implication*, is defined as follows:*

$$a \rightarrow b \;\triangleq\; |a](\ulcorner b).$$

Hence $a \rightarrow b$ characterizes the set of points from which no computation as described by a may lead outside the domain of b. If a and b are tests then (5) and stability of domain show that $a \rightarrow b$ evaluates to $\neg a + b$, so that both the name "implication" and the symbol are justified. Therefore we also use the convention from Boolean algebra that $+$ and $\cdot$ bind more tightly than $\rightarrow$.

By (2) and (4), we have, for $p, q \in \mathsf{test}(K)$,

$$p \leq a \rightarrow q \;\Leftrightarrow\; p \cdot a \cdot \neg q \leq 0. \tag{8}$$

Both of theses formulas may therefore serve as the definition of validity of the Hoare triple $\{p\}\ a\ \{q\}$.

Further useful properties of test implication are collected in

Lemma 2.14 *Let* p *be a test.*

(a)	$1 \rightarrow a = \ulcorner a$.	
(b)	$a \rightarrow 1 = 1$.	
(c)	$a \rightarrow b \cdot \ulcorner c = a \rightarrow b \cdot c$	*(Domain Absorption).*
(d)	$a + b \rightarrow c = (a \rightarrow c) \cdot (b \rightarrow c)$	*(Antidistributivity).*
(e)	$a \cdot b \rightarrow c = a \rightarrow (b \rightarrow c)$	*(Currying).*
(f)	$a \rightarrow p \cdot b = (a \rightarrow p) \cdot (a \rightarrow b) = (a \rightarrow b) \cdot (a \rightarrow p)$	*(Conjunctivity).*
(g)	$(p \cdot a \rightarrow b) \cdot p = (a \rightarrow b) \cdot p$	*(Modus Ponens).*

(h) $(a \to p \cdot b) \cdot a = (a \to p \cdot b) \cdot a \cdot p$ *(Test Propagation).*

PROOF.

(a)
$$\begin{aligned} & 1 \to a \\ = & \quad \{\![\text{ Definitions 2.10, 2.11 2.13 }]\!\} \\ & \neg\ulcorner(1 \cdot \neg\ulcorner a) \\ = & \quad \{\![\text{ neutrality, stability of domain }]\!\} \\ & \neg\neg\ulcorner a \\ = & \quad \{\![\text{ involution }]\!\} \\ & \ulcorner a \end{aligned}$$

(b)
$$\begin{aligned} & a \to 1 \\ = & \quad \{\![\text{ Definitions 2.10, 2.11 2.13 }]\!\} \\ & \neg\ulcorner(a \cdot \neg 1) \\ = & \quad \{\![\text{ Boolean algebra }]\!\} \\ & \neg\ulcorner(a \cdot 0) \\ = & \quad \{\![\text{ strictness of } \cdot \text{ and domain }]\!\} \\ & \neg 0 \\ = & \quad \{\![\text{ Boolean algebra }]\!\} \\ & 1 \end{aligned}$$

(c)
$$\begin{aligned} & a \to b \cdot c \\ = & \quad \{\![\text{ Definition 2.13 }]\!\} \\ & |a]\ulcorner(b \cdot c) \\ = & \quad \{\![\text{ (loc) }]\!\} \\ & |a]\ulcorner(b \cdot \ulcorner c) \\ = & \quad \{\![\text{ Definition 2.13 }]\!\} \\ & a \to b \cdot \ulcorner c \end{aligned}$$

(d) Immediate from (6).

(e) Immediate from (7).

(f) Immediate from (c) and (3).

(g)
$$\begin{aligned} & (p \cdot a \to b) \cdot p \\ = & \quad \{\![\text{ (e) }]\!\} \\ & (p \to (a \to b)) \cdot p \\ = & \quad \{\![\text{ for tests } \to \text{ coincides with implication,} \\ & \quad \text{modus ponens of Boolean algebra }]\!\} \\ & (a \to b) \cdot p \end{aligned}$$

(h) We first note that substituting $a \to p$ and p for p and q in (8) yields

$(a \to p) \cdot a \cdot \neg p = 0$. Hence

$$(a \to p) \cdot a = (a \to p) \cdot a \cdot p + (a \to p) \cdot a \cdot \neg p = (a \to p) \cdot a \cdot p.$$

Now the claim follows by (f). □

The property of domain absorption is frequently used in the special case where $b = 1$; it then reads $a \to \ulcorner c = a \to c$.

3 The Basic Demonic Operators

3.1 Refinement Ordering, Demonic Join and Demonic Meet

We now define a partial ordering, called the *refinement ordering*. This ordering induces an upper semilattice, called the *demonic semilattice*. The associated operations are demonic join ($\sqcup$), demonic meet ($\sqcap$) and demonic composition ($\circ$). Again, we generalize from the case of relation algebra to arbitrary KAs. For more details on relational demonic semantics and demonic operators, see [3–5,9,10,33].

Definition 3.1 *We say that an element a* refines *an element b [21], denoted by $a \sqsubseteq b$, iff $\ulcorner b \leq \ulcorner a \ \wedge \ \ulcorner b \cdot a \leq b$.*

It is easy to show that $\sqsubseteq$ is indeed a partial ordering.

Since the following theorem employs meets, we first quote the following properties [26].

Lemma 3.2 *In a test semiring K, the following hold for all $a, b, c \in K$ and all $p, q \in \mathsf{test}(K)$.*

(a) If $a \sqcap b$ exists then $p \cdot (a \sqcap b) = p \cdot a \sqcap b = p \cdot a \sqcap p \cdot b$.
(b) $(p \cdot q) \cdot a = p \cdot a \sqcap q \cdot a$.
(c) $p \cdot q = 0 \Rightarrow p \cdot a \sqcap q \cdot a = 0$.
(d) If $b \leq a$ then $p \cdot b = b \sqcap p \cdot a$. In particular, if K has a greatest element $\top$ then $p \cdot b = b \sqcap p \cdot \top$.

From this we obtain

Corollary 3.3 *If $a \sqcap b$ exists then $\ulcorner b \cdot a \sqcap \ulcorner a \cdot b = a \sqcap b$.*

PROOF. Using Lemma 3.2(a) four times and (d1) twice, we obtain $\ulcorner b \cdot a \sqcap \ulcorner a \cdot b = \ulcorner a \cdot \ulcorner b \cdot (a \sqcap b) = \ulcorner a \cdot a \sqcap \ulcorner b \cdot b = a \sqcap b$. □

Moreover,

Lemma 3.4 *For $p, q \in \mathsf{test}(K)$ with $p \cdot q = 0$ and $a, b, c \in K$,*

$$p \cdot a \leq q \cdot b + c \;\Leftrightarrow\; p \cdot a \leq p \cdot c.$$

PROOF. ($\Rightarrow$) $p \cdot a = p \cdot p \cdot a \leq p \cdot (q \cdot b + c) = p \cdot q \cdot b + p \cdot c = 0 + p \cdot c$.
($\Leftarrow$) $p \cdot a \leq p \cdot c \leq c \leq q \cdot b + c$. □

Now we can prove the following properties.

Theorem 3.5 *The partial order $\sqsubseteq$ respects existing suprema and infima w.r.t $\leq$ in the following sense.*

(a) If a non-empty subset $L \subseteq K$ has a $\leq$-supremum $\bigsqcup L$ and $p \triangleq \bigsqcap(a : a \in L : \ulcorner a)$ exists, then L also has a $\sqsubseteq$-supremum, called its demonic join*, viz.*

$$\bigsqcup L \;=\; p \cdot \bigsqcup L \qquad \text{with} \qquad \ulcorner(\bigsqcup L) = p.$$

In particular, $\sqsubseteq$ induces an upper semilattice.

(b) $a \sqsubseteq b \;\Leftrightarrow\; a \sqcup b = b$.

(c) If the $\leq$-infimum $a \sqcap b$ of a and b exists and satisfies the condition $\ulcorner(a \sqcap b) = \ulcorner a \cdot \ulcorner b$, then a and b have a $\sqsubseteq$-infimum, called their demonic meet*, viz.*

$$a \sqcap\!\!\sqcap b \;=\; (a \sqcap b) + \neg\ulcorner a \cdot b + \neg\ulcorner b \cdot a \qquad \text{with} \qquad \ulcorner(a \sqcap\!\!\sqcap b) = \ulcorner a + \ulcorner b.$$

Otherwise, their $\sqsubseteq$-infimum does not exist. As a particular case, if $\ulcorner a \cdot \ulcorner b = 0$ then $a \sqcap\!\!\sqcap b = a + b$.

In relational terms, the existence condition for $\sqcap\!\!\sqcap$ simply means that for each argument in the intersection of their domains, a and b have to agree for at least one result value.

PROOF.

(a) The claim about the domain of $\sqcup L$ is immediate. We show that $a \sqcup b$ is the $\sqsubseteq$-supremum of a and b. This is the special case of the overall assertion for binary $\leq$-suprema, which are guaranteed to exist in every idempotent semiring. The generalization to arbitrary sets that have $\leq$-suprema is straightforward.

$$
\begin{aligned}
& a \sqsubseteq c \wedge b \sqsubseteq c \\
\Leftrightarrow \quad & \{\![\text{ definition of } \sqsubseteq \ ]\!\} \\
& \ulcorner c \leq \ulcorner a \wedge \ulcorner c \cdot a \leq c \wedge \ulcorner c \leq \ulcorner b \wedge \ulcorner c \cdot b \leq c \\
\Leftrightarrow \quad & \{\![\text{ infimum, supremum and distributivity }]\!\} \\
& \ulcorner c \leq \ulcorner a \cdot \ulcorner b \wedge \ulcorner c \cdot (a + b) \leq c \\
\Leftrightarrow \quad & \{\![\text{ infimum }]\!\} \\
& \ulcorner c \leq \ulcorner a \cdot \ulcorner b \wedge \ulcorner c \cdot \ulcorner a \cdot \ulcorner b \cdot (a + b) \leq c \\
\Leftrightarrow \quad & \{\![\text{ definition of } \sqcup \text{ and domain of } a \sqcup b \ ]\!\} \\
& \ulcorner c \leq \ulcorner (a \sqcup b) \wedge \ulcorner c \cdot (a \sqcup b) \leq c \\
\Leftrightarrow \quad & \{\![\text{ definition of } \sqsubseteq \ ]\!\} \\
& a \sqcup b \sqsubseteq c
\end{aligned}
$$

(b) ($\Rightarrow$) By the assumption, distributivity, domain and Boolean algebra,

$$a \sqcup b = \ulcorner a \cdot \ulcorner b \cdot (a + b) = \ulcorner b \cdot (a + b) = \ulcorner b \cdot a + b = b.$$

($\Leftarrow$) By definition, distributivity and idempotence of tests,

$$a \sqcup b = b \Leftrightarrow \ulcorner a \cdot \ulcorner b \cdot (a + b) = b \Leftrightarrow \ulcorner b \cdot a + \ulcorner a \cdot b = b.$$

This immediately implies $\ulcorner b \cdot a \leq b$. Moreover, by distributivity of domain and (loc) we obtain

$$\ulcorner b \cdot \ulcorner a + \ulcorner a \cdot \ulcorner b = \ulcorner b,$$

which is equivalent to $\ulcorner b \leq \ulcorner a$.

(c) First, we show the domain property.

$$
\begin{aligned}
& \ulcorner (a \sqcap b) \\
= \quad & \{\![\text{ definition, distributivity and (loc) }]\!\} \\
& \ulcorner (a \sqcap b) + \neg \ulcorner a \cdot \ulcorner b + \neg \ulcorner b \cdot \ulcorner a \\
= \quad & \{\![\text{ assumption }]\!\} \\
& \ulcorner a \cdot \ulcorner b + \neg \ulcorner a \cdot \ulcorner b + \neg \ulcorner b \cdot \ulcorner a \\
= \quad & \{\![\text{ Boolean algebra }]\!\} \\
& \ulcorner a + \ulcorner b
\end{aligned}
$$

Second, we derive an equivalent to the property of being a $\sqsubseteq$-lower-bound for a and b.

$$
\begin{aligned}
& c \sqsubseteq a \wedge c \sqsubseteq b \\
\Leftrightarrow \quad & \{\![\text{ definition of } \sqsubseteq \ ]\!\} \\
& \ulcorner a \leq \ulcorner c \wedge \ulcorner a \cdot c \leq a \wedge \ulcorner b \leq \ulcorner c \wedge \ulcorner b \cdot c \leq b \\
\Leftrightarrow \quad & \{\![\text{ supremum and for all } a, b \in K, p \in \mathsf{test}(K), \\
& \quad a \leq b \ \Leftrightarrow \ p \cdot a \leq p \cdot b \wedge \neg p \cdot a \leq \neg p \cdot b \ ]\!\} \\
& \ulcorner a + \ulcorner b \leq \ulcorner c \wedge \\
& \ulcorner a \cdot \ulcorner b \cdot c \leq \ulcorner b \cdot a \wedge \ulcorner a \cdot \neg \ulcorner b \cdot c \leq \neg \ulcorner b \cdot a \wedge
\end{aligned}
$$

$$
\begin{array}{ll}
& \lceil a \cdot \lceil b \cdot c \leq \lceil a \cdot b \wedge \neg\lceil a \cdot \lceil b \cdot c \leq \neg\lceil a \cdot b \\
\Leftrightarrow & \quad \{\![\text{ infimum and Corollary 3.3 }]\!\} \\
& \lceil a + \lceil b \leq \lceil c \wedge \lceil a \cdot \lceil b \cdot c \leq a \sqcap b \wedge \\
& \lceil a \cdot \neg\lceil b \cdot c \leq \neg\lceil b \cdot a \wedge \neg\lceil a \cdot \lceil b \cdot c \leq \neg\lceil a \cdot b \\
\Leftrightarrow & \quad \{\![\text{ domain import/export and previous line imply } \lceil a \cdot \lceil b \leq \lceil(a \sqcap b): \\
& \qquad \lceil a \cdot \lceil b = \lceil a \cdot \lceil b \cdot (\lceil a + \lceil b) \leq \lceil a \cdot \lceil b \cdot \lceil c = \lceil(\lceil a \cdot \lceil b \cdot c) \leq \lceil(a \sqcap b) \ ]\!\} \\
& \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \wedge \lceil a + \lceil b \leq \lceil c \wedge \lceil a \cdot \lceil b \cdot c \leq a \sqcap b \wedge \\
& \lceil a \cdot \neg\lceil b \cdot c \leq \neg\lceil b \cdot a \wedge \neg\lceil a \cdot \lceil b \cdot c \leq \neg\lceil a \cdot b \\
\Leftrightarrow & \quad \{\![\lceil a + \lceil b = \lceil a \cdot \lceil b + \lceil a \cdot \neg\lceil b + \neg\lceil a \cdot \lceil b \text{ and distributivity }]\!\} \\
& \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \wedge \lceil a + \lceil b \leq \lceil c \wedge \\
& (\lceil a + \lceil b) \cdot c \leq (a \sqcap b) + \neg\lceil b \cdot a + \neg\lceil a \cdot b \\
\Leftrightarrow & \quad \{\![\text{ expression for } a \sqcap\!\!\!- b \text{ given in the statement }]\!\} \\
& \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \wedge \lceil a + \lceil b \leq \lceil c \wedge (\lceil a + \lceil b) \cdot c \leq a \sqcap\!\!\!- b \\
\Leftrightarrow & \quad \{\![\text{ the proof above shows } \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \Rightarrow \lceil a + \lceil b = \lceil(a \sqcap\!\!\!- b) \ ]\!\} \\
& \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \wedge \lceil(a \sqcap\!\!\!- b) \leq \lceil c \wedge \lceil(a \sqcap\!\!\!- b) \cdot c \leq a \sqcap\!\!\!- b \\
\Leftrightarrow & \quad \{\![\text{ definition of } \sqsubseteq\!\!\!\!- \ ]\!\} \\
& \lceil a \cdot \lceil b \leq \lceil(a \sqcap b) \wedge c \sqsubseteq\!\!\!\!- a \sqcap\!\!\!- b
\end{array}
$$

Assume now $\lceil a \cdot \lceil b = 0$ and consider any common lower bound c of a and b w.r.t. $\leq$. By isotonicity of domain then $\lceil c \leq \lceil a$ and $\lceil c \leq \lceil b$, hence $\lceil c \leq \lceil a \cdot \lceil b = 0$, so that $c = 0$ by full strictness of domain. Therefore, $a \sqcap b = 0$ and the claim follows from the just derived formula for the demonic meet by the assumption $\lceil a \cdot \lceil b = 0$, Boolean algebra and (llp).

□

3.2 Demonic Composition

Definition 3.6 *Let a and b be elements of a domain semiring. The* demonic composition *of a and b, denoted by $a \boxdot b$, is defined as* $a \boxdot b \triangleq (a \rightarrow b) \cdot a \cdot b$.

In the algebra of relations, a pair (s, t) belongs to $a \boxdot b$ if and only if it belongs to $a \cdot b$ and there is no possibility of reaching from s via a an element u that does not belong to the domain of b. For example, with $a \triangleq \{(0,0),(0,1),(1,2)\}$ and $b \triangleq \{(0,0),(2,3)\}$, one finds that $a \boxdot b = \{(1,3)\}$; the pair $(0,0)$, which belongs to $a \cdot b$, does not belong to $a \boxdot b$, since $(0,1) \in a$ and 1 is not in the domain of b. Note that we assign to $\boxdot$ and $\cdot$ the same binding power.

A first consequence of the definition is

Lemma 3.7 $\lceil(a \boxdot b) = (a \rightarrow b) \cdot \lceil a$.

PROOF.

$$
\begin{array}{ll}
 & \ulcorner(a \mathbin{\triangleright} b) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & \ulcorner((a \rightarrow b) \cdot a \cdot b) \\
= & \quad \{\![\text{ (loc) }]\!\} \\
 & \ulcorner((a \rightarrow b) \cdot a \cdot \ulcorner b) \\
= & \quad \{\![\text{ (d1) twice and test propagation }]\!\} \\
 & \ulcorner((a \rightarrow b) \cdot a) \\
= & \quad \{\![\text{ import/export }]\!\} \\
 & (a \rightarrow b) \cdot \ulcorner a
\end{array}
$$

□

A fundamental property is shown in

Theorem 3.8 *Demonic composition is associative.*

PROOF.

$$
\begin{array}{ll}
 & (a \mathbin{\triangleright} b) \mathbin{\triangleright} c \\
= & \quad \{\![\text{ definition of } \mathbin{\triangleright}]\!\} \\
 & (((a \rightarrow b) \cdot a \cdot b \rightarrow c)) \cdot (a \rightarrow b) \cdot a \cdot b \cdot c \\
= & \quad \{\![\text{ modus ponens }]\!\} \\
 & (a \cdot b \rightarrow c) \cdot (a \rightarrow b) \cdot a \cdot b \cdot c \\
= & \quad \{\![\text{ currying }]\!\} \\
 & (a \rightarrow (b \rightarrow c)) \cdot (a \rightarrow b) \cdot a \cdot b \cdot c \\
= & \quad \{\![\text{ weak distributivity }]\!\} \\
 & (a \rightarrow (b \rightarrow c) \cdot b) \cdot a \cdot b \cdot c \\
= & \quad \{\![\text{ (d1), test propagation with } b, c, \ulcorner c \text{ for } a, b, p, \\
 & \qquad \text{and domain absorption }]\!\} \\
 & (a \rightarrow (b \rightarrow c) \cdot b \cdot c) \cdot a \cdot b \cdot c \\
= & \quad \{\![\text{ test propagation }]\!\} \\
 & (a \rightarrow (b \rightarrow c) \cdot b \cdot c) \cdot a \cdot (b \rightarrow c) \cdot b \cdot c \\
= & \quad \{\![\text{ definition of } \mathbin{\triangleright}]\!\} \\
 & a \mathbin{\triangleright} (b \mathbin{\triangleright} c)
\end{array}
$$

□

Theorem 3.9 *Demonic composition $\mathbin{\triangleright}$ preserves binary demonic joins in both arguments and hence is $\sqsubseteq$-isotone.*

PROOF. Left argument:

$$
\begin{array}{ll}
 & (a \rhd c) \sqcup (b \rhd c) \\
= & \quad \{\![\text{ definitions and Lemma 3.7 }]\!\} \\
 & (a \to c) \cdot \ulcorner a \cdot (b \to c) \cdot \urcorner b \cdot ((a \to c) \cdot a \cdot c + (b \to c) \cdot b \cdot c) \\
= & \quad \{\![\text{ distributivity, idempotence of tests and rearrangement }]\!\} \\
 & (a \to c) \cdot (b \to c) \cdot \ulcorner a \cdot \urcorner b \cdot (a + b) \cdot c \\
= & \quad \{\![\text{ antidistributivity (Lemma 2.14(d)) }]\!\} \\
 & (a + b \to c) \cdot \ulcorner a \cdot \urcorner b \cdot (a + b) \cdot c \\
= & \quad \{\![\text{ modus ponens (Lemma 2.14(g) }]\!\} \\
 & (\ulcorner a \cdot \urcorner b \cdot (a + b) \to c) \cdot \ulcorner a \cdot \urcorner b \cdot (a + b) \cdot c \\
= & \quad \{\![\text{ definition }]\!\} \\
 & ((a \sqcup b) \to c) \cdot (a \sqcup b) \cdot c \\
= & \quad \{\![\text{ definition }]\!\} \\
 & (a \sqcup b) \rhd c.
\end{array}
$$

Right argument:

$$
\begin{array}{ll}
 & (a \rhd b) \sqcup (a \rhd c) \\
= & \quad \{\![\text{ definitions and Lemma 3.7 }]\!\} \\
 & (a \to b) \cdot \ulcorner a \cdot (a \to c) \cdot \ulcorner a \cdot ((a \to b) \cdot a \cdot b + (a \to c) \cdot a \cdot c) \\
= & \quad \{\![\text{ distributivity, idempotence of tests, Boolean algebra} \\
 & \quad \text{and rearrangement }]\!\} \\
 & (a \to b) \cdot (a \to c) \cdot \ulcorner a \cdot a \cdot (b + c) \\
= & \quad \{\![\text{ domain (d1) }]\!\} \\
 & (a \to b) \cdot (a \to c) \cdot a \cdot (b + c) \\
= & \quad \{\![\text{ isotonicity and Boolean algebra }]\!\} \\
 & (a \to b) \cdot (a \to c) \cdot (a \to b + c) \cdot a \cdot (b + c) \\
= & \quad \{\![\text{ domain absorption (Lemma 2.14(c)) twice }]\!\} \\
 & (a \to \urcorner b) \cdot (a \to \ulcorner c) \cdot (a \to b + c) \cdot a \cdot (b + c) \\
= & \quad \{\![\text{ conjunctivity (Lemma 2.14(f)) }]\!\} \\
 & (a \to \urcorner b \cdot \ulcorner c \cdot (b + c)) \cdot a \cdot (b + c) \\
= & \quad \{\![\text{ test propagation (Lemma 2.14(h)) }]\!\} \\
 & (a \to \urcorner b \cdot \ulcorner c \cdot (b + c)) \cdot a \cdot \urcorner b \cdot \ulcorner c \cdot (b + c) \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & a \rhd (b \sqcup c).
\end{array}
$$

□

Theorem 3.10 $\ulcorner a \cdot \urcorner b = 0 \;\Rightarrow\; (a + b) \rhd c = a \rhd c + b \rhd c.$

PROOF.

$$
\begin{aligned}
& (a+b) \mathbin{\triangleright} c \\
= \quad & \{\![\text{ definitions }]\!\} \\
& (a+b \to c) \cdot (a+b) \cdot c \\
= \quad & \{\![\text{ antidistributivity (Lemma 2.14(d)) and distributivity }]\!\} \\
& (a \to c) \cdot (b \to c) \cdot a \cdot c + (a \to c) \cdot (b \to c) \cdot b \cdot c \\
= \quad & \{\![\text{ commutativity of tests, and definitions }]\!\} \\
& (b \to c) \cdot (a \mathbin{\triangleright} c) + (a \to c) \cdot (b \mathbin{\triangleright} c).
\end{aligned}
$$

Now, $\ulcorner a \cdot \ulcorner b = 0$ implies $\ulcorner a \leq \neg \ulcorner b \leq b \to c$ and hence, by Lemma 3.7,

$$(b \to c) \cdot \ulcorner(a \mathbin{\triangleright} c) = (b \to c) \cdot \ulcorner a \cdot (a \to c) = \ulcorner a \cdot (a \to c) = \ulcorner(a \mathbin{\triangleright} c),$$

so that $(b \to c) \cdot (a \mathbin{\triangleright} c) = a \mathbin{\triangleright} c$ by (llp). Symmetrically, $(a \to c) \cdot (b \mathbin{\triangleright} c) = b \mathbin{\triangleright} c$. □

For the next theorem we need a notion of determinacy [15].

Definition 3.11 *We call* a deterministic *iff* $\mathrm{MD}(a)$ *holds, where*

$$\mathrm{MD}(a) \stackrel{\Delta}{\Leftrightarrow} |a\rangle \leq |a]. \tag{9}$$

This reflects a well-known characterization of determinacy that is used in modal correspondence theory (see e.g. [29]).

We quote from [15]:

Lemma 3.12 *All tests are deterministic. If* a *is deterministic and* $b \leq a$*, then* b *is deterministic as well.*

Now we can show

Theorem 3.13 a *deterministic* $\Rightarrow a \mathbin{\triangleright} b = a \cdot b$.

PROOF.

$$
\begin{aligned}
& a \mathbin{\triangleright} b = a \cdot b \\
\Leftrightarrow \quad & \{\![\text{ definition of } \triangleright \text{ and (llp) }]\!\} \\
& \ulcorner(a \cdot b) \leq a \to b
\end{aligned}
$$

$\Leftrightarrow$ {[(loc) and Definitions 2.10 and 2.13]}
$|a\rangle\ulcorner b \leq |a]\ulcorner b$
$\Leftarrow$ {[definition of MD (9)]}
$\mathrm{MD}(a)$ $\Box$

The following stronger notion (see [15]) entails $\mathrm{MD}(a)$, and so in (a) of the above theorem also the premise $\mathrm{CD}(a)$ could be used.

Definition 3.14 *Element a is* domain-deterministic *iff* $\mathrm{CD}(a)$ *holds, where*

$$\mathrm{CD}(a) \stackrel{\Delta}{\Leftrightarrow} \forall(b : b \leq a : b = \ulcorner b \cdot a) \qquad \textit{(characterization by domain).}$$

In [15] the implication $\mathrm{CD}(a) \Rightarrow \mathrm{MD}(a)$ was shown for the narrower setting of MKAs with complete Boolean algebras as carriers. Here we show a quick proof in MKA. Using the definitions and Boolean algebra we can transform $\mathrm{MD}(a)$ equivalently into $\forall(p :: \ulcorner(a \cdot p) \cdot \ulcorner(a \cdot \neg p) = 0)$. Now, assuming $\mathrm{CD}(a)$, we calculate

$\ulcorner(a \cdot p) \cdot \ulcorner(a \cdot \neg p) = 0$
$\Leftrightarrow$ {[import/export]}
$\ulcorner(\ulcorner(a \cdot p) \cdot a \cdot \neg p) = 0$
$\Leftrightarrow$ {[strictness of domain]}
$\ulcorner(a \cdot p) \cdot a \cdot \neg p = 0$
$\Leftrightarrow$ {[by $a \cdot p \leq a$ and $\mathrm{CD}(a)$]}
$a \cdot p \cdot \neg p = 0$
$\Leftrightarrow$ {[Boolean algebra and strictness of $\cdot$]}
true.

4 Iteration: Modal Kleene and Omega Algebras

So far we have only given the semantics of loop-free programs. We now introduce operators for describing iteration of program parts.

4.1 Fixed Points

We recall a few basic facts about fixed points that will be used in the axiomatization of the iteration operators. First, we state a slight generalization of the well-known Knaster/Tarski fixed point theorem.

Definition 4.1 *Consider a partial order $(M, \leq)$ and a function $f : M \to M$. If the set of all fixed points of f has a least (greatest) element, this element is denoted by $\mu(f)$ ($\nu(f)$).*

Theorem 4.2 *Let $(M, \leq)$ be a partial order and $f : M \to M$ be $\leq$-isotone.*

(a) If $u \in M$ is the least pre-fixed point of f, i.e., if $f(u) \leq u \wedge f(x) \leq x \Rightarrow u \leq x$ then $u = \mu_f$, i.e., u is also the least fixed point of f.
(b) Analogously, if the greatest post-fixed point of f exists then it is also the greatest fixed point ν_f of f.
(c) If also $g : M \to M$ is isotone and satisfies $f \leq g$, i.e., $\forall(x :: f(x) \leq g(x))$, then also $\mu_f \leq \mu_g$ and $\nu_f \leq \nu_g$, provided these elements exist.
(d) If $(M, \leq)$ is even a complete lattice then $\mu(f)$ and $\nu(f)$ exist and satisfy

$$\begin{aligned} \mu(f) &= \textstyle\bigsqcap(x : f(x) = x : x) &= \textstyle\bigsqcap(x : f(x) \leq x : x), \\ \nu(f) &= \textstyle\bigsqcup(x : f(x) = x : x) &= \textstyle\bigsqcup(x : x \leq f(x) : x). \end{aligned}$$

In the case of a Boolean lattice, least and greatest fixed points can be related via the notion of a *dual* function.

Definition 4.3 *Let f be a function on a Boolean lattice. The* dual function *of f, denoted $f^{\#}$, is defined by $f^{\#}(x) \triangleq \neg f(\neg x)$.*

Lemma 4.4 *Let f be a function on a Boolean lattice. If $\mu(f)$ exists then also $\nu(f^{\#})$ exists and $\nu(f^{\#}) = \neg\mu(f)$. Likewise, if $\nu(f)$ exists then also $\mu(f^{\#})$ exists and $\mu(f^{\#}) = \neg\nu(f)$.*

4.2 Finite Iteration: Modal Kleene Algebras

While modal semirings suffice for some applications, others require an explicit notion of iteration. This is achieved by extending idempotent semirings to Kleene algebras.

Definition 4.5 *A* Kleene algebra *[19] is a structure $(K, ^*)$ such that K is an idempotent semiring and the* star * *satisfies, for $a, b, c \in K$, the* unfold *and*

induction laws

$$1 + a \cdot a^* \leq a^*, \tag{$*$-1}$$
$$1 + a^* \cdot a \leq a^*, \tag{$*$-2}$$
$$b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c, \tag{$*$-3}$$
$$b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c. \tag{$*$-4}$$

Therefore, a^* is the least pre-fixed point and the least fixed point of the mappings $\lambda x \,.\, a \cdot x + b$ and $\lambda x \,.\, x \cdot a + b$, and hence the star is isotone with respect to the natural ordering.

Two important properties that follow from these axioms are the laws

$$b \cdot a \leq a \cdot c \;\Rightarrow\; b^* \cdot a \leq a \cdot c^*, \qquad a \cdot b \leq c \cdot a \;\Rightarrow\; a \cdot b^* \leq c^* \cdot a. \tag{10}$$

All our examples LAN, REL and PAT can be made into KAs by setting $a^* \triangleq \sum_{i \in \mathbb{N}} a^i$.

Definition 4.6 *(a) A* Kleene algebra with tests (KAT) *[20] is a test semiring* $(K, \mathsf{test}(K))$ *such that* K *is a* KA.
(b) If the underlying test semiring of a KAT K *is a domain (codomain) semiring, we speak of a* KA with domain (codomain)*, briefly* ⌜-(⌝-)KA.
(c) Finally, a modal Kleene algebra (MKA) *is a KAT in which the underlying test semiring is modal.*

Examples of MKAs are again LAN, REL and PAT.

In a KAT, for all $p \in \mathsf{test}(K)$ we have that $p^* = 1$. Moreover, the angelic semantics of a loop can be given as

$$\mathsf{while}\ p\ \mathsf{do}\ a \triangleq (p \cdot a)^* \cdot \neg p.$$

This way, by the star induction axioms, $\mathsf{while}\ p\ \mathsf{do}\ a$ is the least fixed point of the function

$$\lambda x \,.\, \mathsf{if}\ p\ \mathsf{then}\ a \cdot x\ \mathsf{else}\ \mathsf{skip}.$$

Using the star induction axioms, one can show the following induction principle for the diamond operator in an MKA (cf. [11]):

$$|a\rangle p + q \leq p \;\Rightarrow\; |a^*\rangle q \leq p. \tag{11}$$

Moreover we have (see again [11])

$$p \cdot a \cdot \neg p \leq 0 \;\Leftrightarrow\; p \cdot a^* \cdot \neg p \leq 0. \tag{12}$$

We now introduce infinite iteration of an element and the notion of progressive finiteness.

Definition 4.7 *An* omega algebra *[7] is a structure* $(K, {}^{\omega})$ *such that* K *is a* KA *and the* infinite iteration a^{ω} *of an element* a *satisfies the following unfold and co-induction axioms.*

$$a^{\omega} \leq a \cdot a^{\omega}, \tag{13}$$

$$c \leq a \cdot c + b \Rightarrow c \leq a^{\omega} + a^{*} \cdot b, \tag{14}$$

for all $a, b, c \in K$*. A* modal omega algebra *is an omega algebra in which the underlying* KA *is an* MKA*.*

Consequently, a^{ω} is the greatest post-fixed point and the greatest fixed point of $\lambda x \,.\, a \cdot x$, and hence the omega operator is isotone w.r.t the natural order. Moreover, every omega algebra has the greatest element $\top = 1^{\omega}$ and for every a the element a^{ω} is a vector, i.e., an element v satisfying $v \cdot \top = \top$.

In the algebra of relations, the complement of a^{ω} is also known as the *initial part* [30] of a. It characterizes the set of points s_0 such that there is no infinite chain $s_0, s_1, s_2, \ldots$, with $(s_i, s_{i+1}) \in a$, for all $i \geq 0$. Since we do not assume general complements to exist we will characterize this set in a different way.

Definition 4.8 *An element* a *is said to be* progressively finite *[30] iff* $a^{\omega} = 0$*.*

In the algebra of relations, progressive finiteness of a relation R is the same as well-foundedness of $R^{\smile}$.

We now list some useful properties of infinite iteration.

Theorem 4.9 *Let* a *and* b *be elements of an omega algebra.*

(a) If b *is progressively finite and* $a \leq b$ *then also* a *is progressively finite.*
(b) In a modal omega algebra, $\neg\ulcorner(a^{\omega}) \cdot a$ *is progressively finite.*
(c) Let $f(x) \triangleq a \cdot x + b$*. If* a *is progressively finite, then* f *has a unique fixed point, viz.* $a^{*} \cdot b$ *[2].*
(d) $a^{\omega} = a^{*} \cdot a^{\omega}$*.*

PROOF.

(a) Immediate from isotonicity of the omega operator.
(b) Set $b \triangleq \neg\ulcorner(a^{\omega}) \cdot a$. Since $b \leq a$ we get $b^{\omega} \leq a^{\omega}$ and hence $\ulcorner(b^{\omega}) \leq \ulcorner(a^{\omega})$.

On the other hand, by (d2) and stability of domain

$$\ulcorner(b^\omega) \;=\; \ulcorner(b \cdot b^\omega) \;=\; \ulcorner(\neg\ulcorner(a^\omega) \cdot a \cdot b^\omega) \;\leq\; \ulcorner(\neg\ulcorner(a^\omega)) \;=\; \neg\ulcorner(a^\omega).$$

So $\ulcorner(b^\omega) \leq \ulcorner(a^\omega) \cdot \neg\ulcorner(a^\omega) = 0$ and hence $b^\omega = 0$.

(c) This is immediate, since the star and omega axioms imply $\mu(f) = a^* \cdot b$ and $\nu(f) = \mu(f) + a^\omega$.

(d) $a^* \cdot a^\omega = a^* \cdot a \cdot a^\omega = a \cdot a^* \cdot a^\omega$, so that $a^* \cdot a^\omega \leq a^\omega$ by the co-induction axiom (14) used with $b = 0$. Since also $a^\omega \leq a^* \cdot a^\omega$ holds, equality follows. □

4.4 Iteration at the Test Level

We have already noted that $p^* = 1$ for all tests p of a KAT. So, finite iteration at the test level is not interesting. However, one can use an analogue of omega iteration at the level of tests: If the test algebra of an MKA is complete, the Knaster/Tarski theorem implies that for every element a the greatest fixed point $\nu(|a\rangle)$ exists, since $|a\rangle$ is isotone. It turns out that $\nu(|a\rangle)$ is more suitable for termination analysis than a^ω, as will be seen in the next section.

If the test algebra is not complete, $\nu(|a\rangle)$ may not exist. Instead, one can axiomatize it, similarly to the omega operation, by [12]

$$\nu(|a\rangle) \leq |a\rangle\, \nu(|a\rangle), \tag{15}$$

$$p \leq |a\rangle p + q \Rightarrow p \leq \nu(|a\rangle) + |a^*\rangle q. \tag{16}$$

In the sequel we will also use its dual:

Definition 4.10 *Assume an* MKA K *such that* $\nu(|a\rangle)$ *exists for all elements* a*. Then we set* $\mathcal{T}_\ulcorner(a) \triangleq \neg\nu(|a\rangle) = \mu(x :: a \to x)$.

The second equation follows from Lemma 4.4, since any fixed point of $\lambda x \,.\, a \to x$ needs to be a test. By the correspondence with the modal box operator mentioned in Section 2.4, $\mathcal{T}_\ulcorner(a) = \mu(|a]\rangle)$. In the propositional μ-calculus, this is known as the *halting predicate* (see, e.g., [17]). It is easy to check that $\neg\ulcorner(a^\omega)$ is a fixed point of $(x :: a \to x)$. Hence,

Corollary 4.11 *Assume an omega* MKA *such that* $\nu(|a\rangle)$ *exists for all elements* a*.*

(a) $\mathcal{T}_\ulcorner(a) \leq \neg\ulcorner(a^\omega)$.
(b) $\mathcal{T}_\ulcorner(a) \cdot a^\omega = 0$.
(c) $\mathcal{T}_\ulcorner(a) \cdot a$ *is progressively finite.*

PROOF. (a) is immediate from the least fixed point property of $\mathcal{T}_{\ulcorner}(a)$, and (b) follows from (a) by Boolean algebra and (d1).

For (c), by isotonicity of $\_^{\omega}$ we get $(\mathcal{T}_{\ulcorner}(a) \cdot a)^{\omega} \leq (\neg\ulcorner(a^{\omega}) \cdot a)^{\omega} = 0$ using Theorem 4.9(b). □

We now determine the least and greatest fixed points of test-level recursions that are analogous to star and omega iteration. To exhibit dualities, we state the theorem in the notation of modal operators, avoiding test implication $\rightarrow$.

Theorem 4.12 *Assume an* MKA K *such that* $\nu(|a\rangle)$ *exists for all* $a \in K$.

Let p *be a test and set* $\quad h(x) \triangleq |a\rangle\ulcorner x + p, \quad k(x) \triangleq |a]\ulcorner x - p.$

(a) $x \in \mathsf{test}(K) \Rightarrow h(x) = \neg k(\neg x)$.
(b) $\mu(h) = |a^*\rangle p$.
(c) $\nu(h) = |a^*\rangle p + \nu(|a\rangle)$.
(d) $|a^*]\ulcorner a \leq \nu(|a\rangle)$.
(e) $\mu(k) = |a^*]\neg p - \nu(|a\rangle)$.
(f) $\nu(k) = |a^*]\neg p$.

PROOF. Part (a) is clear.
For the remaining properties we note that $h(x) \leq 1$ and $k(x) \leq 1$ for any $x \in K$. Hence, any fixed point of h or k is a test. Because the tests constitute a Boolean algebra, one can consider h and k to be functions on the set of tests for the purpose of calculating fixed points. That said, part (b) follows by a straightforward calculation that shows $\ulcorner(a^* \cdot p)$ to be a fixed point of h and by the induction law (11). Symmetrically, part (c) follows from (16). Next, by part (a) h and k are dual in the sense of Definition 4.3. Therefore Lemma 4.4 gives parts (e) and (f).
For part (d), we first show for all $q \in \mathsf{test}(K)$ that $\ulcorner a \cdot |a]q \leq |a\rangle q$; the proof uses shunting, distributivity and Boolean algebra:

$$\ulcorner a \cdot |a]q \leq |a\rangle q \;\Leftrightarrow\; \ulcorner a \leq |a\rangle q + |a\rangle\neg q \;\Leftrightarrow$$
$$\ulcorner a \leq |a\rangle(q + \neg q) \;\Leftrightarrow\; \ulcorner a \leq \ulcorner a.$$

Now, we establish the claim by the coinduction law (16) showing that $|a^*]\ulcorner a$ is expanded by $|a\rangle$; this employs star unfold, antidisjunctivity, compositionality of box and the above derivation:

$$|a^*]\ulcorner a \;=\; |1 + a \cdot a^*]\ulcorner a \;=\; \ulcorner a \cdot |a]|a^*]\ulcorner a \;\leq\; |a\rangle|a^*]\ulcorner a.$$

□

We now reconsider the question whether a program admits infinite execution sequences. To this end we abstract a notion of termination for modal semirings from set-theoretic relations. A similar characterisation has been used, for instance, in [16] for related structures. A set-theoretic relation $R \subseteq A \times A$ on a set A is well-founded if there are no infinitely descending R-chains, that is, no infinite chains $x_0, x_1, \ldots$ such that $(x_{i+1}, x_i) \in R$. It is Noetherian if there are no infinitely ascending R-chains, i.e., no infinite chains $x_0, x_1, \ldots$ such that $(x_i, x_{i+1}) \in R$. Thus R is *not* well-founded if there is a non-empty set $P \subseteq A$ (denoting the infinite chain) such that for all $x \in P$ there exists some $y \in P$ with $(y, x) \in R$. Equivalently, therefore, P is contained in the image of P under R, i.e., $P \subseteq (P\,;R)^{\urcorner}$. Consequently, if R *is* well-founded, then only the empty set may satisfy this condition.

Abstracting to a modal semiring K we say that a is *well-founded* if

$$p \leq \langle a|p \Rightarrow p \leq 0 \tag{17}$$

for all $p \in \mathsf{test}(K)$. Dually, a is *Noetherian* if for all $p \in \mathsf{test}(K)$,

$$p \leq |a\rangle p \Rightarrow p \leq 0. \tag{18}$$

Note that by de Morgan duality, a is Noetherian iff, for all $p \in \mathsf{test}(K)$,

$$|a]p \leq p \Rightarrow 1 \leq p. \tag{19}$$

Let us look at these definitions from another angle. According to the standard definition, a relation R on a set A is well-founded iff every non-empty subset of A has an R-minimal element. In a $^{\urcorner}$-semiring K the minimal part of $p \in \mathsf{test}(K)$ w.r.t. some $a \in K$ can algebraically be characterised as $p - \langle a|p$, i.e., as the set of points that have no a-predecessor in p. So, by contraposition, the well-foundedness condition holds iff for all $p \in \mathsf{test}(K)$

$$p - \langle a|p \;\leq\; 0 \;\Rightarrow\; p \leq 0,$$

which by simple Boolean algebra can be transformed into (17).

It is easy to prove some of the well-known properties of well-founded and Noetherian relations in modal Kleene algebra [11]. First, 0 is the only Noetherian test. Second, the property of being Noetherian is downward closed. Third, every Noetherian element is irreflexive and non-dense, provided it is non-trivial. Fourth, an element is Noetherian iff its transitive closure is, but no reflexive transitive closure is Noetherian. Finally, Noethericity of a sum implies Noethericity of its components, whereas the converse direction does not hold in general.

With the help of $\nu(|a\rangle)$ we can rephrase Noethericity more concisely as

$$\nu(|a\rangle) = 0. \tag{20}$$

As an immediate consequence of this we obtain

Corollary 4.13 *Define, for fixed $q \in \mathsf{test}(K)$ and $a \in K$, the function $f : \mathsf{test}(K) \to \mathsf{test}(K)$ by $f(p) = q + |a\rangle p$. If $\nu(|a\rangle)$ exists and a is Noetherian then f has the unique fixed point $|a^*\rangle q$.*

We now consider the relation between Noethericity and progressive finiteness.

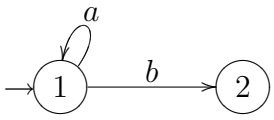
Lemma 4.14 *Every Noetherian element of a modal omega algebra K is progressively finite, but not conversely.*

This is simply illustrated in LAN. Since there are no infinite words, $a^\omega = 0$ for all a with $\varepsilon \notin a$. But for all $a \neq 0$, the operator $|a\rangle$ is the identity, and so $\nu(|a\rangle) = 1 \neq 0$. This reflects that a^ω talks about actual infinity, whereas $\nu(|a\rangle)$ captures potential infinity, and indeed every word in LAN can be iterated indefinitely. Thus omega algebra does not capture the standard notion of termination fully.

5 The Semantics of Nondeterministic Loops

5.1 Intuition and Notation

A general nondeterministic loop is best described by a graph of the form



It may "execute" a as long as the intermediate states remain in the domain of a and it may exit if a state in the domain of b is reached. The domains of a and b need not be disjoint. Since a may be nondeterministic, it can take a starting state s to many successor states. If among these there exists a state outside the domains of a and b (abnormal termination), then in the demonic view s must be excluded from the domain of the loop semantics. Hence, in addition to $\mathcal{T}_\Gamma(a)$, we introduce a test $\mathcal{P}(a, b)$ ($\mathcal{P}$ stands for *p*roper) that characterizes the states from which no abnormal termination is possible.

We now define the corresponding semantic functions formally. Let a and b be elements. The abbreviations f, φ, $\mathcal{P}(a,b)$, s_ν and s_μ are defined as follows:

$$\left.\begin{array}{rcll} f(x) & \triangleq & a \cdot x + b, & s_\nu \triangleq \mathcal{P}(a,b) \cdot \nu(f), \\ \varphi(x) & \triangleq & (a \to x) \cdot f(x), & s_\mu \triangleq \mathcal{P}(a,b) \cdot \mathcal{T}_\Gamma(a) \cdot \mu(f), \\ \mathcal{P}(a,b) & \triangleq & a^* \to \nu(f), & \end{array}\right\} \tag{21}$$

where we know from Sections 4.2 and 4.3 that $\mu(f) = a^* \cdot b$ and $\nu(f) = \mu(f) + a^\omega$. The test for proper progress $\mathcal{P}(a,b)$ expresses that after finitely iterating a, it is only possible to iterate a infinitely often or to reach b after again finitely iterating a (infinite looping and proper termination are possible, but not improper termination).

The element s_μ, *which we take as the semantics of the loop*, is the restriction of the angelic loop semantics $a^* \cdot b$ to $\mathcal{P}(a,b)$ and $\mathcal{T}_\Gamma(a)$. Hence the domain of s_μ represents the set of states from which proper termination is guaranteed.

5.2 Properties of the Semantics

We want to show that s_μ and s_ν are the least and greatest fixed points of φ, respectively. We first deal with the greatest fixed point.

Theorem 5.1 $\nu(\varphi) = s_\nu$.

PROOF. We use Theorem 4.2(b) and show that s_ν is the greatest post-fixed point of φ.

(1) All post-fixed points of φ are below s_ν.

$$\begin{array}{ll} & x \leq \varphi(x) \\ \Leftrightarrow & \quad \{\![\text{ definition of } \varphi \ ]\!\} \\ & x \leq (a \to x) \cdot f(x) \\ \Leftrightarrow & \quad \{\![\text{ Lemma 2.7 }]\!\} \\ & \ulcorner x \leq a \to x \ \wedge \ x \leq f(x) \\ \Rightarrow & \quad \{\![\text{ greatest fixed point of } f \ ]\!\} \\ & \ulcorner x \leq a \to x \ \wedge \ x \leq \nu(f) \\ \Leftrightarrow & \quad \{\![\text{ domain absorption (Lemma 2.14(c)), (8) and (12) }]\!\} \\ & \ulcorner x \leq a^* \to x \ \wedge \ x \leq \nu(f) \\ \Rightarrow & \quad \{\![\text{ isotonicity of } \to \text{ in its right argument }]\!\} \\ & \ulcorner x \leq a^* \to \nu(f) \ \wedge \ x \leq \nu(f) \end{array}$$

$$
\begin{array}{ll}
\Leftrightarrow & \{\![\text{ Lemma 2.7 }]\!\} \\
& x \leq (a^* \to \nu(f)) \cdot \nu(f) \\
\Leftrightarrow & \{\![\text{ definition of } s_\nu \ ]\!\} \\
& x \leq s_\nu
\end{array}
$$

(2) s_ν is a post-fixed point of φ.

$$
\begin{array}{ll}
& \varphi(s_\nu) \\
= & \{\![\text{ definition of } \varphi \text{ and } s_\nu \ ]\!\} \\
& \Big(a \to \Big(\mathcal{P}(a,b) \cdot \nu(f)\Big)\Big) \cdot \Big(a \cdot \mathcal{P}(a,b) \cdot \nu(f) + b\Big) \\
= & \{\![\text{ test propagation (Lemma 2.14(h)) }]\!\} \\
& \Big(a \to \Big(\mathcal{P}(a,b) \cdot \nu(f)\Big)\Big) \cdot \Big(a \cdot \nu(f) + b\Big) \\
= & \{\![\text{ definition of } f \text{ and } f(\nu(f)) = \nu(f) \ ]\!\} \\
& \Big(a \to \Big(\mathcal{P}(a,b) \cdot \nu(f)\Big)\Big) \cdot \nu(f) \\
= & \{\![\text{ conjunctivity (Lemma 2.14(f)) }]\!\} \\
& \Big(a \to \mathcal{P}(a,b)\Big) \cdot \Big(a \to \nu(f)\Big) \cdot \nu(f) \\
= & \{\![\text{ definition of } \mathcal{P}(a,b) \text{ and currying (Lemma 2.14(e)) }]\!\} \\
& (a \cdot a^* \to \nu(f)) \cdot (a \to \nu(f)) \cdot \nu(f) \\
= & \{\![\ a \cdot a^* \to \nu(f) \leq a \to \nu(f) \text{ by left antitonicity of } \to \ ]\!\} \\
& (a \cdot a^* \to \nu(f)) \cdot \nu(f) \\
\geq & \{\![\to \text{ is antitone in its left argument }]\!\} \\
& (a^* \to \nu(f)) \cdot \nu(f) \\
= & \{\![\text{ definition of } s_\nu \text{ and definition of } \mathcal{P}(a,b) \ ]\!\} \\
& s_\nu
\end{array}
$$

□

Theorem 5.2 *(a)* $\mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a) \leq \ulcorner(\mu(f))$.
(b) $\mathcal{P}(a,b) \leq \ulcorner(\nu(f))$.
(c) $\ulcorner s_\mu = \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a)$ *and* $\ulcorner s_\nu = \mathcal{P}(a,b)$.
(d) $s_\mu = \mathcal{T}_\ulcorner(a) \cdot s_\nu$.

PROOF.

(a) We show $\mathcal{T}_\ulcorner(a) \leq \ulcorner(\mu(f)) + \neg\mathcal{P}(a,b)$, which is equivalent to the claim by shunting.

$$
\begin{array}{ll}
& \ulcorner(\mu(f)) + \neg\mathcal{P}(a,b) \\
= & \{\![\text{ definitions of } f \text{ and } \mathcal{P}(a,b) \text{ (21), and that of } \to \text{ (2.13) }]\!\} \\
& \ulcorner(a^* \cdot b) + \ulcorner(a^* \cdot \neg\ulcorner(\nu(f)) \\
= & \{\![\ a^* \cdot a^* = a^*, \text{ (loc) and } \nu(f) = a^\omega + a^* \cdot b \ ]\!\} \\
& \ulcorner(a^* \cdot \ulcorner(a^* \cdot b)) + \ulcorner(a^* \cdot \neg\ulcorner(a^\omega + a^* \cdot b))
\end{array}
$$

$$
\begin{array}{ll}
= & \{\![\text{ additivity of domain, distributivity and de Morgan }]\!\} \\
& \ulcorner(a^* \cdot (\ulcorner(a^* \cdot b) + \neg\ulcorner(a^\omega) \cdot \neg\ulcorner(a^* \cdot b))) \\
= & \{\![\text{ Boolean algebra }]\!\} \\
& \ulcorner(a^* \cdot (\ulcorner(a^* \cdot b) + \neg\ulcorner(a^\omega))) \\
\geq & \{\![\text{ isotonicity }]\!\} \\
& \ulcorner(a^* \cdot \neg\ulcorner(a^\omega)) \\
\geq & \{\![1 \leq a^* \text{ and isotonicity }]\!\} \\
& \ulcorner(\neg\ulcorner(a^\omega)) \\
\geq & \{\![\text{ stability of domain and Corollary 4.11(a) }]\!\} \\
& \mathcal{T}_\ulcorner(a)
\end{array}
$$

(b) We show $1 \leq \ulcorner(\nu(f)) + \neg\mathcal{P}(a,b)$, which is equivalent, by shunting.

$$
\begin{array}{ll}
& \ulcorner(\nu(f)) + \neg\mathcal{P}(a,b) \\
= & \{\![\text{ (21), Definition 2.13 and } \nu(f) = a^\omega + a^* \cdot b \text{ }]\!\} \\
& \ulcorner(a^\omega + a^* \cdot b) + \ulcorner(a^* \cdot \neg\ulcorner(a^\omega + a^* \cdot b)) \\
= & \{\![\text{ } a^* \cdot a^* = a^*, \text{ Theorem 4.9(d), (loc) and distributivity }]\!\} \\
& \ulcorner(a^* \cdot \ulcorner(a^\omega + a^* \cdot b)) + \ulcorner(a^* \cdot \neg\ulcorner(a^\omega + a^* \cdot b)) \\
= & \{\![\text{ additivity of domain and distributivity }]\!\} \\
& \ulcorner(a^* \cdot (\ulcorner(a^\omega + a^* \cdot b) + \neg\ulcorner(a^\omega + a^* \cdot b))) \\
= & \{\![\text{ Boolean algebra }]\!\} \\
& \ulcorner(a^* \cdot 1) \\
= & \{\![\text{ } \ulcorner(a^*) \geq \ulcorner 1 = 1 \text{ }]\!\} \\
& 1
\end{array}
$$

(c) We give the proof for s_μ. That for s_ν is similar, except that it uses part (b) instead of (a).

$$
\begin{array}{ll}
& \ulcorner s_\mu \\
= & \{\![\text{ (21) }]\!\} \\
& \ulcorner(\mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a) \cdot a^* \cdot b) \\
= & \{\![\text{ import/export }]\!\} \\
& \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a) \cdot \ulcorner(a^* \cdot b) \\
= & \{\![\text{ definition of } f, \text{ (a) and Boolean algebra }]\!\} \\
& \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a)
\end{array}
$$

(d)

$$
\begin{array}{ll}
& \mathcal{T}_\ulcorner(a) \cdot s_\nu \\
= & \{\![\text{ definition of } s_\nu \text{ (21) }]\!\} \\
& \mathcal{T}_\ulcorner(a) \cdot \mathcal{P}(a,b) \cdot \nu(f) \\
= & \{\![\text{ } \nu(f) = a^\omega + a^* \cdot b \text{ }]\!\} \\
& \mathcal{T}_\ulcorner(a) \cdot \mathcal{P}(a,b) \cdot (a^\omega + a^* \cdot b)
\end{array}
$$

$$
\begin{array}{ll}
= & \quad \{\![\text{ Corollary 4.11(b) }]\!\} \\
& \mathcal{T}_{\ulcorner}(a) \cdot \mathcal{P}(a,b) \cdot a^* \cdot b \\
= & \quad \{\![\text{ definition of } s_\mu \text{ and } f \text{ (21) }]\!\} \\
& s_\mu
\end{array}
$$

□

In the following theorem, we show that s_μ is a fixed point of φ.

Theorem 5.3 $\varphi(s_\mu) = s_\mu$.

PROOF.

$$
\begin{array}{ll}
& \varphi(s_\mu) \\
= & \quad \{\![\text{ Theorem 5.2(d) }]\!\} \\
& \varphi(\mathcal{T}_{\ulcorner}(a) \cdot s_\nu) \\
= & \quad \{\![\text{ definition of } \varphi \text{ (21) }]\!\} \\
& (a \rightarrow \mathcal{T}_{\ulcorner}(a) \cdot s_\nu) \cdot (a \cdot \mathcal{T}_{\ulcorner}(a) \cdot s_\nu + b) \\
= & \quad \{\![\text{ test propagation (Lemma 2.14(h)) }]\!\} \\
& (a \rightarrow \mathcal{T}_{\ulcorner}(a) \cdot s_\nu) \cdot (a \cdot s_\nu + b) \\
= & \quad \{\![\text{ conjunctivity (Lemma 2.14(f)) }]\!\} \\
& (a \rightarrow \mathcal{T}_{\ulcorner}(a)) \cdot (a \rightarrow s_\nu) \cdot (a \cdot s_\nu + b) \\
= & \quad \{\![\text{ Definition 4.10, definition of } \varphi \text{ (21) and Theorem 5.1 }]\!\} \\
& \mathcal{T}_{\ulcorner}(a) \cdot s_\nu \\
= & \quad \{\![\text{ Theorem 5.2(d) }]\!\} \\
& s_\mu
\end{array}
$$

□

And now, we determine the domain of $\mu(\varphi)$.

Theorem 5.4 $\ulcorner(\mu(\varphi)) = \mathcal{T}_{\ulcorner}(a) \cdot \mathcal{P}(a,b)$.

PROOF.

$$
\begin{array}{ll}
& \ulcorner(\mu(\varphi)) \\
= & \quad \{\![\text{ definition of } \varphi \text{ (21) }]\!\} \\
& \ulcorner((a \rightarrow \ulcorner(\mu(\varphi))) \cdot (a \cdot \mu(\varphi) + b)) \\
= & \quad \{\![\text{ domain import/export and (loc) }]\!\} \\
& (a \rightarrow \ulcorner(\mu(\varphi))) \cdot \ulcorner(a \cdot \ulcorner(\mu(\varphi)) + b)
\end{array}
$$

$$
\begin{array}{ll}
= & \{\![\text{ domain import/export }]\!\} \\
& \ulcorner((a \to \ulcorner(\mu(\varphi))) \cdot (a \cdot \ulcorner(\mu(\varphi)) + b)) \\
= & \{\![\text{ test propagation (Lemma 2.14(h)) }]\!\} \\
& \ulcorner((a \to \ulcorner(\mu(\varphi))) \cdot (a + b)) \\
= & \{\![\text{ domain import/export }]\!\} \\
& (a \to \ulcorner(\mu(\varphi))) \cdot \ulcorner(a + b)
\end{array}
$$

Hence $\ulcorner(\mu(\varphi))$ is a fixed point of $\varphi_\ulcorner(x) \triangleq (a \to x) \cdot \ulcorner(a+b) = (|a]\ulcorner x) \cdot \ulcorner(a+b)$. By Theorem 4.12(e) and Definition 4.10, $\mu(\varphi_\ulcorner) = \mathcal{T}_\ulcorner(a) \cdot (a^* \to a + b)$. Hence, by the derivation above, Theorem 5.3, Theorem 5.2(c) and isotonicity (using $a^* \to \nu(f) \leq a^* \to a + b$), we get

$$
\mathcal{T}_\ulcorner(a) \cdot (a^* \to a+b) \;\leq\; \ulcorner(\mu(\varphi)) \;\leq\; \ulcorner s_\mu \;=\; \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a) \;\leq\; \mathcal{T}_\ulcorner(a) \cdot (a^* \to a+b),
$$

so that all expressions are equal and thus $\ulcorner(\mu(\varphi)) = \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a)$. □

The following theorem uniquely characterizes the least fixed point of φ by a simple condition and shows that s_μ is the least fixed point of φ. It also shows that a similar condition cannot be given for the greatest fixed point, the reason being that other elements can be fixed points and have a domain equal to that of the greatest fixed point.

Theorem 5.5 *Recall Equations (21). For all elements a and c,*

(a) $c = \mu(\varphi) \;\Leftrightarrow\; \varphi(c) = c \wedge \ulcorner c \leq \mathcal{T}_\ulcorner(a)$,
(b) $c = \nu(\varphi) \;\Rightarrow\; \varphi(c) = c \wedge \mathcal{P}(a,b) \leq \ulcorner c$, *and the reverse implication does not hold,*
(c) $\mu(\varphi) = s_\mu$.

PROOF.

(a) ($\Rightarrow$) Assume $c = \mu(\varphi)$. The property $\varphi(c) = c$ then obviously follows. From Theorem 5.3 and Theorem 4.2(a), we get $c \leq s_\mu$ and hence, by Theorem 5.2(c), $\ulcorner c \leq \ulcorner s_\mu = \mathcal{P}(a,b) \cdot \mathcal{T}_\ulcorner(a) \leq \mathcal{T}_\ulcorner(a)$.

($\Leftarrow$) Assume $\varphi(c) = c$ and $\ulcorner c \leq \mathcal{T}_\ulcorner(a)$. Theorems 5.4, 5.1 and 5.2(c) imply $\mathcal{T}_\ulcorner(a) \cdot \mathcal{P}(a,b) \leq \ulcorner c \leq \mathcal{P}(a,b)$. Hence $\ulcorner c = \mathcal{T}_\ulcorner(a) \cdot \mathcal{P}(a,b)$. This is used in the following derivation.

$$
\begin{array}{ll}
& c \\
= & \{\![\text{ definition of } \varphi \text{ (21) }]\!\} \\
& (a \to c) \cdot (a \cdot c + b) \\
= & \{\![\text{ domain absorption (Lemma 2.14(c)) }]\!\}
\end{array}
$$

$$
\begin{array}{ll}
& (a \to \mathcal{T}_{\ulcorner}(a) \cdot \mathcal{P}(a,b)) \cdot (a \cdot c + b) \\
= & \quad \{\![\text{ conjunctivity (Lemma 2.14(f)) }]\!\} \\
& (a \to \mathcal{T}_{\ulcorner}(a)) \cdot (a \to \mathcal{P}(a,b)) \cdot (a \cdot c + b) \\
= & \quad \{\![\text{ Definition 4.10 }]\!\} \\
& \mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot (a \cdot c + b) \\
= & \quad \{\![\text{ distributivity }]\!\} \\
& \mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot a \cdot c \ + \ \mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot b
\end{array}
$$

By Corollary 4.11(c) and Theorem 4.9(a), $\mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot a$ is progressively finite. Invoking Corollary 4.9(c) shows that the function

$$(x :: \mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot a \cdot x \ + \ \mathcal{T}_{\ulcorner}(a) \cdot (a \to \mathcal{P}(a,b)) \cdot b)$$

has a unique fixed point. Thus all elements c such that $\varphi(c) = c$ and $\ulcorner c \leq \mathcal{T}_{\ulcorner}(a)$ are equal. But $\mu(\varphi)$ is such an element, as we have shown above (part $\Rightarrow$). We conclude that $c = \mu(\varphi)$.

(b) Assume $c = \nu(\varphi)$. The property $\varphi(c) = c$ then follows. From Theorem 5.1, we get $c = \nu(\varphi) = s_\nu$ and hence, by Theorem 5.2(c), $\ulcorner c = \ulcorner(s_\nu) = \mathcal{P}(a,b)$.

The reverse implication does not hold, as the following counter-example shows. Take $\varphi(x) \triangleq (1 \to x) \cdot (x + 1)$ (i.e., $a = 1$ and $b = 1$ in (21). It is easy to verify that 1 is a fixed point of φ and that $\top$ is the greatest fixed point. Also, $\mathcal{P}(a,b) = 1 \leq \top$. Both $c \triangleq 1$ and $c \triangleq \top$ satisfy $\varphi(c) = c \wedge \mathcal{P}(a,b) \leq \ulcorner c$, but only $\top$ is the greatest fixed point.

(c) By Theorem 5.3, $s_\mu = \varphi(s_\mu)$. By Theorem 5.2(c), $\ulcorner s_\mu \leq \mathcal{T}_{\ulcorner}(a)$. Now the claim is a consequence of part (a) of this theorem. □

Lemma 5.6 *If* $\ulcorner a \cdot \ulcorner b = 0$, *then* $\varphi(x) = a \,\square\, x \sqcap b$.

PROOF.

$$
\begin{array}{ll}
& a \,\square\, x \sqcap b \\
= & \quad \{\![\text{ definition of } \square \text{ (Definition 3.6) }]\!\} \\
& (a \to x) \cdot a \cdot x \sqcap b \\
= & \quad \{\![\text{ Theorem 3.5(c) }]\!\} \\
& (a \to x) \cdot a \cdot x \ + \ b \\
= & \quad \{\![\ (a \to x) \ + \ \neg(a \to x) \ = \ 1 \text{ and distributivity }]\!\} \\
& (a \to x) \cdot a \cdot x \ + \ (a \to x) \cdot b \ + \ \neg(a \to x) \cdot b \\
= & \quad \{\![\ \neg(a \to x) \cdot b = \ulcorner(a \cdot \neg\ulcorner x) \cdot b \leq \ulcorner a \cdot b = 0 \text{ and distributivity }]\!\} \\
& (a \to x) \cdot (a \cdot x + b) \\
= & \quad \{\![\text{ definition of } \varphi \text{ }]\!\} \\
& \varphi(x)
\end{array}
$$

□

Lemma 5.6 justifies why we are talking about a demonic star operator.

5.3 Relating Angelic and Demonic Semantics

In the sequel, we will show that the element s_μ is the greatest fixed point with respect to $\sqsubseteq$ of the function φ (Equations (21)). But first, we show

Lemma 5.7 *The function φ is isotonic wrt $\sqsubseteq$.*

PROOF. Assume $x \sqsubseteq y$. First, using domain import/export, (loc) and isotonicity, we get

$$\ulcorner\varphi(y) \leq \ulcorner\varphi(x) \;\Leftrightarrow\; (a \to y) \cdot \ulcorner(a \cdot \ulcorner y + b) \;\leq\; (a \to x) \cdot \ulcorner(a \cdot \ulcorner x + b) \;\Leftarrow\; \ulcorner y \leq \ulcorner x.$$

Second,

$$\begin{array}{ll} & \ulcorner\varphi(y) \cdot \varphi(x) \\ = & \quad \{\![\text{ domain import/export }]\!\} \\ & (a \to y) \cdot \ulcorner(a \cdot y + b) \cdot (a \to x) \cdot (a \cdot x + b) \\ \leq & \quad \{\![\text{ isotonicity }]\!\} \\ & (a \to y) \cdot (a \cdot x + b) \\ = & \quad \{\![\text{ test propagation (Lemma 2.14(h)) }]\!\} \\ & (a \to y) \cdot (a \cdot \ulcorner y \cdot x + b) \\ \leq & \quad \{\![\text{ hypothesis } \ulcorner y \cdot x \leq y \ ]\!\} \\ & (a \to y) \cdot (a \cdot y + b) \\ = & \quad \{\![\text{ definition of } \varphi \ ]\!\} \\ & \varphi(y) \end{array}$$

□

Now we show the main result of this section.

Theorem 5.8 *The element s_μ (Equations (21)) is the $\sqsubseteq$-greatest fixed point of φ, that is, $s_\mu = \nu_{\sqsubseteq}(\varphi)$.*

PROOF. Let w be an arbitrary fixed point of φ. Using Theorem 5.5(c), the definition of s_μ (21), and Theorems 5.2(b,d) and 5.1, we obtain

$$s_\mu = \ulcorner s_\mu \cdot s_\mu \leq \ulcorner s_\mu \cdot w \leq \ulcorner s_\mu \cdot \nu(\varphi) \leq \mathcal{T}_\ulcorner(a) \cdot s_\nu = s_\mu,$$

and hence $w \sqsubseteq s_\mu$. □

In other words, the least fixed point of φ wrt $\leq$ is equal to the greatest fixed point of the same function φ wrt $\sqsubseteq$. Indeed, the refinement relation $w \sqsubseteq s_\mu$ between an arbitrary fixed point w of φ and s_μ is special in that the restriction of w to $\ulcorner s_\mu$ fully coincides with s_μ, i.e., there is no reduction of nondeterminacy. This holds because the domain of s_μ is below $\mathcal{T}_\ulcorner(a)$ and hence the restriction to it excludes all the infinite behaviour but nothing else, so that the full finite behaviour as given by s_μ remains.

6 Application

In Mills's approach, the semantics w of a deterministic loop `do g` $\rightarrow$ `C od` is given as the least fixed point (wrt $\leq$) of the function

$$w_{gc}(x) \;\triangleq\; g \cdot c \cdot x + \neg g,$$

where the test g is the semantics of the loop guard `g` and the element c is the semantics of the loop body `C`.

Lemma 6.1 *If the loop body c is deterministic, then*

$$w_{gc}(x) \;=\; (g \cdot c \rightarrow x) \cdot (g \cdot c \cdot x + \neg g) \;=\; g \,\square\, c \,\square\, x \;\sqcap\; \neg g.$$

PROOF. First we note that by Lemma 3.12 also $g \cdot c$ is deterministic. Next, by the definitions, Boolean algebra and (d2),

$$\neg g \leq g \cdot c \rightarrow x. \tag{22}$$

Now, the first claimed equation is established by (llp) if we can show that $\ulcorner(w_{gc}(x)) \leq g \cdot c \rightarrow x$. This holds, since

$$\begin{array}{ll} & \ulcorner(w_{gc}(x)) \leq g \cdot c \rightarrow x \\ \Leftrightarrow & \quad \{\![\text{ definitions, distributivity and stability }]\!\} \\ & \ulcorner(g \cdot c \cdot x) + \neg g \leq g \cdot c \rightarrow x \\ \Leftrightarrow & \quad \{\![\text{ (loc) and join }]\!\} \\ & \ulcorner(g \cdot c \cdot \ulcorner x) \leq g \cdot c \rightarrow x \;\wedge\; \neg g \leq g \cdot c \rightarrow x \\ \Leftrightarrow & \quad \{\![\text{ definitions and (22) }]\!\} \\ & |g \cdot c\rangle \ulcorner x \leq |g \cdot c] \ulcorner x \\ \Leftrightarrow & \quad \{\![\text{ determinacy of } g \cdot c \,]\!\} \\ & \mathsf{true} \end{array}$$

For the second claimed equation we calculate

$$
\begin{array}{ll}
 & (g \cdot c \rightarrow x) \cdot (g \cdot c \cdot x + \neg g) \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & (g \cdot c \rightarrow x) \cdot g \cdot c \cdot x + (g \cdot c \rightarrow x) \cdot \neg g \\
= & \quad \{\![\text{ definition of } \boxdot \text{ and (22) }]\!\} \\
 & (g \cdot c) \boxdot x + \neg g \\
= & \quad \{\![\text{ Theorem 3.5(c), since } \ulcorner((g \cdot c) \boxdot x) \leq g \\
 & \qquad \text{by Lemma 3.7 and import/export }]\!\} \\
 & (g \cdot c) \boxdot x \sqcap \neg g \\
= & \quad \{\![\text{ Lemma 3.12, Theorem 3.13 and Theorem 3.8 }]\!\} \\
 & g \boxdot c \boxdot x \sqcap \neg g
\end{array}
$$

□

Hence, in this case, the demonic and angelic semantics coincide, as expected. Moreover, under mild additional assumptions on the underlying KA, the semantics of the loop is a deterministic element as well [15].

Calculating the semantics of a loop is difficult, but *showing the correctness* of any candidate element is much easier. For deterministic programs, Mills [22,23] has described a checking method known as the *while statement verification rule*. In a nondeterministic context, the abstraction is calculated by considering the worst behavior of the program (*demonic semantics*) [33]. Given a loop condition and a loop body, Theorem 5.5 (with $a \triangleq g \cdot c$ and $b \triangleq \neg g$; notice that $\ulcorner a \cdot \ulcorner b = 0$) can be used to verify if an element w is indeed the semantics of the loop.

The following example is rather contrived, but it is simple and fully illustrates the various cases that may happen. Consider the following loop, where the variable n ranges over the set of integers [10,34]:

Example 6.2 *Consider the program*

```
do n > 0 → if n = 1 → n := 1   [] n = 1 → n := −3
            [] n = 3 → n := 2   [] n = 3 → n := −1
            [] n ≥ 4 → n := n−4
           fi
od
```

Notice that all $n > 0$ such that $n \bmod 4 = 1$ may lead to termination with a final value $n' = -3$, but may also lead to an infinite loop via the value $n = 1$; therefore these initial values of n do not belong to the domain of the element w that is the demonic semantics of the loop. Note also that all $n > 0$ such that $n \bmod 4 = 3$ may lead to termination with a final value $n' = -1$, but may also lead to a value $n = 2$, for which the loop body is not defined (by the

semantics of if fi); these n do not belong to the domain of w. Because they also lead to $n = 2$, all $n > 0$ such that $n \bmod 4 = 2$ do not belong to the domain of w.

The semantics of the loop guard in the concrete MKA REL is given by

$$g = \{n > 0 \wedge n' = n\} \qquad (\text{whence } \neg g = \{n \leq 0 \wedge n' = n\}).$$

(For readability reasons, for any predicate P, instead of $\{(n, n') \mid P(n, n')\}$ we simply write $\{P(n, n')\}$.) The semantics of the loop body is

$$\begin{aligned} c \;=\;& \{n = 1 \wedge n' = n\} \mathbin{\triangledown} (\{n' = 1\} \sqcup \{n' = -3\}) \\ & \sqcap \{n = 3 \wedge n' = n\} \mathbin{\triangledown} (\{n' = 2\} \sqcup \{n' = -1\}) \\ & \sqcap \{n \geq 4 \wedge n' = n\} \mathbin{\triangledown} \{n' = n - 4\} \\ =\;& \{(n = 1 \wedge (n' = 1 \vee n' = -3) \\ & \vee \;\; (n = 3 \wedge (n' = 2 \vee n' = -1) \\ & \vee \;\; (n \geq 4 \wedge n' = n - 4)\}. \end{aligned}$$

By Lemma 3.12 and Theorem 3.13, $g \mathbin{\triangledown} c = g \cdot c = c$. Using Theorem 5.5(a), we show that the semantics of the loop is

$$w \;\triangleq\; \{(n \leq 0 \wedge n' = n) \;\vee\; (n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0)\}.$$

The condition $\varphi(w) = w$ of Theorem 5.5(a) follows from straightforward calculations. The second condition $\ulcorner w \leq \mathcal{T}_{\ulcorner}(g \cdot c)$ can be established informally by noting that the domain of w is $\{n \leq 0 \vee n \bmod 4 = 0\}$, and that there is no infinite sequence by $g \cdot c$ for any n in the domain of w.

A more satisfactory way to show $\ulcorner w \leq \mathcal{T}_{\ulcorner}(g \cdot c)$ is to calculate $\mathcal{T}_{\ulcorner}(g \cdot c)$. However, because $\mathcal{T}_{\ulcorner}(g \cdot c)$ characterizes the domain of guaranteed termination of the associated loop, there is no systematic way to compute it (this would solve the halting problem). To demonstrate termination of the loop from every state in the domain of w, classical proofs based on variant functions or well-founded sets could be given. But formal arguments based on the definition of $\mathcal{T}_{\ulcorner}$ (Definition 4.10) can also be used [10]. The argument in [10] is in fact based on the concept of initial part, but since $\ulcorner a^{\omega} = \nu(|a\rangle)$ in REL, the argument can be adapted to use $\mathcal{T}_{\ulcorner}$.

In this example, Theorem 5.5 was used to *verify* that the guessed semantics w of the loop was correct, given the semantics g of the loop guard and c of the loop body. The theorem can also be used in the other direction. If we are given a specification w, we can guess g and c, and then apply Theorem 5.5 to verify the correctness of the guess. If it is correct, then a loop of the form do g $\rightarrow$ C od, where C is an implementation of c, is correct with respect to w.

7 Conclusion

The paper is another larger case study in applying the novel framework of modal Kleene algebra [13].

It has shown that the relatively strong assumption of a complete Boolean algebra as the overall carrier of the algebra can be replaced by the much weaker assumption of a complete Boolean algebra of tests. This provides additional gain. In the predecessor paper [14], the proof of Theorem 5.8 was non-constructive in that it simply used existence of a least upper bound. This bound need not exist in the MKA setting, and so a more thorough analysis of the structure of the fixed points of the semantic φ became necessary, leading to the explicit expression for the greatest fixed point of φ that was not given in the earlier paper.

Besides this, the modal view exhibits the dualites involved more clearly than the pure Kleene view; this is most evident in the statement of Theorem 4.12.

Also, once again it has turned out that, despite its simple axiomatization, the calculational properties of modal Kleene algebra are very rich and pleasing. Nevertheless, special-purpose abbreviations, like the test implication operator $\rightarrow$, can bring substantial further gain in clarity and concision.

We are convinced that modal Kleene algebra is an easy-to-use formal tool that will have many further applications.

Acknowledgments.

The authors thank Thorsten Ehm, Dexter Kozen and Georg Struth for helpful comments. This research was supported by FCAR (Fonds pour la Formation de Chercheurs et l'Aide à la Recherche, Québec) and NSERC (Natural Sciences and Engineering Research Council of Canada).

References

[1] R. Back and J. von Wright. *Refinement Calculus — A Systematic Introduction.* Springer, 1998.

[2] R. C. Backhouse *et al.* Fixed point calculus. *Information Processing Letters*, 53:131–136, 1995.

[3] R. C. Backhouse and J. van der Woude. Demonic operators and monotype factors. *Mathematical Structures in Computer Science*, 3(4):417–433, 1993.

[4] R. Berghammer and H. Zierer. Relational Algebraic semantics of deterministic and nondeterministic programs. *Theoretical Computer Science*, 43:123–147, 1986.

[5] N. Boudriga, F. Elloumi, and A. Mili, On the lattice of specifications: Applications to a specification methodology. *Formal Aspects of Computing*, 4:544–571, 1992.

[6] C. Brink, W. Kahl, and G. Schmidt, editors. *Relational Methods in Computer Science*. Springer, 1997.

[7] E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Proc. of Mathematics of Program Construction, 5th International Conference, MPC 2000*, volume 1837 of *LNCS*, pages 45–59. Springer, 2000.

[8] J. H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.

[9] J. Desharnais, N. Belkhiter, S. B. M. Sghaier, F. Tchier, A. Jaoua, A. Mili, and N. Zaguia. Embedding a demonic semilattice in a relation algebra. *Theoretical Computer Science*, 149(2):333–360, 1995.

[10] J. Desharnais, A. Mili, and T. T. Nguyen. Refinement and demonic semantics. In [6], Chapter 11, pages 166–183.

[11] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. Technical report 2003-07, Universität Augsburg, Institut für Informatik, June 2003. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2003-7.pdf`.

[12] J. Desharnais, B. Möller, and G. Struth. Termination in modal Kleene algebra. Technical report 2004-04, Universität Augsburg, Institut für Informatik, January 2004. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2004-4.pdf` Revised version to appear in in Proc. IFIP World Computer Congress 2004, Toulouse, August 23—26, 2004, Subconference TCS-Logic. Kluwer 2004.

[13] J. Desharnais, B. Möller, and G. Struth. Applications of modal Kleene algebra — A survey. Technical report DIUL-RR-0401, Département d'informatique et de génie logiciel, Université Laval, Québec, 2004. `http://www.ift.ulaval.ca/~desharnais/Recherche/RR/DIUL-RR-0401.pdf`.

[14] J. Desharnais, B. Möller, and F. Tchier. Kleene under a demonic star. In T. Rus, editor, *Algebraic Methodology and Software Technology*, volume 1816 of *LNCS*, pages 355–370. Springer, 2000.

[15] J. Desharnais and B. Möller. Characterizing determinacy in Kleene algebras. *Information Sciences*, 139(3–4):253–273, December 2001.

[16] R. Goldblatt. An algebraic study of well-foundedness. *Studia Logica*, 44(4):422–437, 1985.

[17] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. The MIT Press, 2000.

[18] E. Hehner. Predicative programming, Parts I and II. *Communications of the ACM*, 27:134–151, 1984.

[19] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.

[20] D. Kozen. Kleene algebras with tests. *ACM Transactions on Programming Languages and Systems*, 19:427–443, 1997.

[21] A. Mili, J. Desharnais, and F. Mili. Relational heuristics for the design of deterministic programs. *Acta Informatica*, 24(3):239–276, 1987.

[22] H. D. Mills. The new math of computer programming. *Communications of the ACM*, 18(1):43–48, 1975.

[23] H. D. Mills, V. R. Basili, J. D. Gannon and R. G. Hamlet. *Principles of Computer Programming. A Mathematical Approach.* Allyn and Bacon, Inc., 1987.

[24] B. Möller. Typed Kleene algebras. Technical report 1999-8, Universität Augsburg, Institut für Informatik, December 1999. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/1999-8.pdf`

[25] B. Möller. Derivation of graph and pointer algorithms. In B. Möller, H.A. Partsch, and S.A. Schuman, editors, *Formal program development*, volume 755 of *LNCS*, pages 123–160. Springer, 1993.

[26] B. Möller. Lazy Kleene algebra. In D. Kozen, editor, *Proc. of Mathematics of Program Construction, 7th International Conference, MPC 2004*, LNCS. Springer, 2004 (to appear). Preliminary version: Technical report No. 2003-17, Institut für Informatik, Universität Augsburg, December 2003. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2003-17.pdf`

[27] B. Möller and G. Struth. Modal Kleene algebra and partial correctness. In *Proc. 10th International Conference on Algebraic Methodology and Software Technology AMAST '2004*, LNCS. Springer, 2004 (to appear). Preliminary version: Technical report No. 2003-08, Institut für Informatik, Universität Augsburg, May 2003. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2003-8.pdf`

[28] T. S. Norvell. Predicative semantics of loops. In R. S. Bird and L. Meertens, editors, *Algorithmic Languages and Calculi*, Chapman & Hall, 1997, pages 415–437.

[29] S. Popkorn: First steps in modal logic. Cambridge University Press 1994.

[30] G. Schmidt and T. Ströhlein. *Relations and Graphs*. EATCS Monographs in Computer Science, Springer, Berlin, 1993.

[31] E. Sekerinski. A calculus for predicative programming. *Second International Conf. on the Mathematics of Program Construction*. R. S. Bird, C. C. Morgan and J. C. P. Woodcock, editors, Oxford, June 1992, volume 669 of *LNCS*, pages 302–322. Springer, 1993.

[32] A. Tarski. On the calculus of relations. *J. of Symbolic Logic*, 6(3):73–89, 1941.

[33] F. Tchier. Sémantiques relationelles demoniaques et vérification de boucles non-déterministes. Ph.D. Thesis, Département de Mathématiques, Université Laval, Canada, 1996.

[34] F. Tchier and J. Desharnais. Applying a generalization of a theorem of Mills to generalized looping structures. Colloquium *Science and Engineering for Software Development*, organized in the memory of Dr. Harlan D. Mills, and affiliated to the *21st International Conference on Software Engineering*, Los Angeles, 18 May 1999, pages 31–38.